Iomega StorCenter px12-400r User Guide

D31621400

Table of Contents

Setting up Your Device 1

Setup Overview 1

Set up My Iomega StorCenter If It's Not Discovered 2

Discovering with Iomega Storage Manager 2

Discovering the Iomega device without the Internet 2

Setup Page 3

Network Connection 4

Connecting the Iomega StorCenter px12-400r to Your Network 4

Network Settings 6

Manually Configuring the Network 7

Bonding NICs 8

VLAN Settings 9

Naming Your Iomega StorCenter px12-400r 10

Configuring Your Iomega StorCenter px12-400r to Use Active Directory 11

Enabling Active Directory Trusted Domains 11

Obtaining Alerts About Your Iomega StorCenter px12-400r 12

Using Your Iomega StorCenter px12-400r in Various Time Zones 13

Setting the Display Language for Your Iomega StorCenter px12-400r 14

Printing Documents 15

Setting up Personal Cloud, Security, and File Sharing 16

Sharing Files 17

Sharing Overview 17

Interfaces for Sharing 17

Shares 18

What are Shares and How Do I Organize Content with Them? 18

Adding Shares 19

Managing Shares 20
Deleting Shares 23
Using Protocols to Share Files 24
What Are Protocols and How Do I Use Them to Share Files? 24
AFP File Sharing for Macs 25
Bluetooth File Sharing 26
FTP File Sharing 27
NFS File Sharing 28
rsync: Synchronizing Files with Another Storage Device or Other Computers 29
TFTP 30
Monitoring Your Device with an SNMP Management Tool 31
WebDAV: Managing Files Using HTTP or HTTPS 32
Windows DFS: Creating a Distributed Windows File System 33
Windows File Sharing 34
Sharing Content through the Home Page 35
Sharing Your Content with the World 35
Adding a Custom Home Page 36
Automatically Sending Content to Multiple People at Once 37
How to Set Up an Email Distribution Active Folder 37
Sharing Content Using Social Media: Overview 38
Managing Your Content 39
Transferring Content to and from Your Iomega StorCenter px12-400r with Copy Jobs 40
Copy Jobs Limitations 40
Getting Content from a USB External Storage Device 41
Safely removing external storage 41
iSCSI: Creating IP-Based Storage Area Networks (SAN) 43
iSCSI Overview 43

Adding iSCSI Drives 44
Enabling iSCSI Drives 44
Connecting to iSCSI Drives 44
Managing iSCSI Drives 46
Creating iSCSI Drives and Adding Them to Volumes 46
Changing Access Permissions 46
Deleting iSCSI Drives 47
Storage Pool Management 49
Understanding How Your Content Is Stored 49
Storage Pools 49
Volumes 49
Adding and Managing Storage Pools 50
Cache Pools 50
To add a Storage Pool 50
Managing Drives 51
Setting Write Caching 51
Applying Global Drive Management Settings 51
Setting Write Caching 51
Applying Global Drive Management Settings 52
Drive status 52
Modifying a Storage Pool 54
Adding and Managing Volumes 55
Shares in Volumes 55
To add a new volume: 55
Deleting a Storage Pool 57
Changing RAID Protection Types 58
Adding New Drives to Your Iomega StorCenter px12-400r 59

Drive Management 61
Managing Drives 61
Setting Write Caching 61
Applying Global Drive Management Settings 61
Setting Write Caching 61
Applying Global Drive Management Settings 62
Drive status 62
Backing up and Restoring Your Content 65
Backup and Restore Overview 65
Backup of Data through RAID Protection 65
Backing up to and Restoring from Your Device 66
Backing up Macs with Time Machine 66
Copy Jobs Overview 67
Backing up Your Device 68
Copy Jobs 68
Backing up with Mozy Backup 76
Restoring Files with Mozy Backup 77
Registering with Avamar for Backup and Restore 78
Backing up with Amazon S3 79
Restoring Files with Amazon S3 80
Backing up with Iomega Personal Cloud 81
Restoring Files with Personal Cloud 82
Securing Your Device and Contents 83
What Is Security and Do I Need It? 83
Enabling Security and Creating an Administrator User 84
Disabling Security 84
Limiting Access to Your Content by Creating Users 85

Users 86
Users Overview 86
Adding Users 87
Managing Users 88
Deleting Users 90
Groups 91
Groups Overview 91
Adding Groups 92
Managing Groups 93
Deleting Groups 94
Using Active Directory Domain to Manage Users and Groups 95
Active Directory Users and Groups Overview 95
Managing Users and Groups with Active Directory 96
Deleting Active Directory Users and Groups 98
Personal Cloud: Accessing Your Device From Anywhere in the World 99
What Is an Iomega Personal Cloud ? 99
Iomega Personal Cloud Key Terms 99
Is My Content Secure? 100
Iomega Personal Cloud Setup Overview 101
Creating an Iomega Personal Cloud 102
Configuring Router Port Forwarding for Personal Cloud 103
Router Port Forwarding 103
Configuring Your Iomega Personal Cloud 105
Enabling Internet Access to the px12-400r 105
Changing Personal Cloud Settings 105
Inviting People onto Your Iomega Personal Cloud 107
Joining a Trusted Device to an Iomega Personal Cloud 108

Managing Trusted Devices on a Personal Cloud 109
Disconnecting Trusted Devices 109
Deleting Trusted Devices 109
Using Copy Jobs with an Iomega Personal Cloud 110
Disabling or Deleting Your Iomega Personal Cloud 111
Accessing Content Using Your Iomega Personal Cloud 112
Informing Users What to Do with Iomega Personal Cloud 113
Sharing Content Using Social Media 115
Sharing Content Using Social Media: Overview 115
Facebook 116
Flickr 117
YouTube 118
Share Content through Iomega Personal Cloud 119
Media Management 121
Media Management Overview 121
Scanning for media content 121
Media Services Capabilities and Limitations 122
Sharing Media Content over the Internet 123
Enabling Internet Access from the Media Server Page 123
Media Aggregation 124
Enabling Media Aggregation 124
Social Media Sharing 125
Streaming Music, Movies, and Pictures 126
Example: Setting up iTunes 126
Example: Setting up Xbox 360 126
Photos 127
Photos Overview 127

Streaming Pictures 128
Creating a Slideshow on the Device Home Page 129
Automatically Resizing Your Photos 130
Getting Pictures from Your Camera 131
Music 132
Music Overview 132
Streaming Music 133
Torrents 134
Torrent Overview 134
Enabling Torrent Downloads 135
Deleting torrent jobs 136
Configuring Your Router for Torrent Downloads 137
Torrent Active Folders 138
Videos 140
Video Capabilities Overview 140
Streaming Movies 141
Adding Applications to Your Device 143
Application Overview 143
Application Manager 144
Starting or stopping an application 144
Adding applications 144
Removing applications 144
Upgrading Your Device 145
Software Updates 145
Manual update process: installing a device software update 145
Recovering Your Device Configuration 147
Copying Your Iomega StorCenter px12-400r Settings to Other Devices 147

Backing up Device Configuration 147
Restoring a Configuration Backup 147
Hardware Management 149
About the Iomega StorCenter px12-400r Components 149
Front Panel 149
Drive Bay Detail 150
Rear Panel 151
Energy Saving 152
Power Down Drives 152
Brightness 152
Wake On LAN 152
Creating A Power Schedule 152
Factory Reset 153
UPS Management 154
Adding New Drives to Your Iomega StorCenter px12-400r 155
Troubleshooting Routers 156
Enabling the DMZ 156
Configuring Port Forwarding on Double NAT Networks 157
Bridging the Secondary Router 157
Bridging the Primary Router 157
Additional Support 159
How to Get Help 159
Support 160
Legal 161
px12-400r Trademark Page 161
Regulatory Information 162
FCC (United States) 162

Canadian Verification 162
CE (European Community) 162
Manufacturer/Responsible Party 162
EU Representative 163
Safety Information 164
Limited Warranty 165
Drives and Media 165
Coverage 165
Excluded Products and Problems 165
Remedies 165
Obtaining Warranty Service 166
Limitations 166
Open Source 167

Setting up Your Device

Setup Overview

Setup with your Iomega StorCenter px12-400r is easy. Remove it from the box, connect it to your network or computer, and power it up. Then, launch a web browser, and enter the setup URL identified in the Quick Install Guide. Iomega Setup launches and displays a message that your px12-400r is online and ready to use.

You then can install client software that includes:

- Iomega Storage Manager
- Twonky Media Server for media aggregation
- Iomega QuikProtect for backups

Iomega Storage Manager is a management tool that helps you discover your px12-400r on your network to simplify access to content on your px12-400r from your computer. It also allows you to add your computer as a trusted device to an Iomega Personal Cloud. Refer to Iomega Storage Manager online help for additional information. Twonky Media Server consolidates all media files on devices on your network and presents them in a unified view. Iomega QuikProtect offers file backup of your computer to an Iomega storage device.

From Iomega Setup, you can optionally create a Personal Cloud or begin using your px12-400r by clicking **Manage My Device**.

How do I ...

set up my px12-400r if it's not discovered
create an Iomega Personal Cloud
set up media aggregation

Set up My Iomega StorCenter If It's Not Discovered

If, after you enter the setup URL identified in the Quick Install Guide, your Iomega device is not discovered, you have two ways of discovering it.

Discovering with Iomega Storage Manager

You can install Iomega Storage Manager from Iomega Setup, which helps you discover your Iomega device on your network.

Discovering the Iomega device without the Internet

You can access your Iomega device device without internet access as described by these methods for Windows pcs or Macs:

- **Windows 7 and Vista** — Click **Start**, **Computer**, **Network**. Under Other Devices, you should see your Iomega device listed. For example, if you have an Iomega device, you can double-click the device labeled Iomega device, and you will see the Iomega StorCenter Console for the Iomega device.
- **Windows XP** — If you have not enabled UPnP Discovery, click **Start**, **Help and Support**. In the Help and Support browser, search for **UPnP**, and follow the steps from "Install the UPnP framework". After UPnP is enabled, open Windows Explorer and in the Folders view, expand My Network Places. You should see your Iomega device listed. For example, if you have an EZ Media device, you can double-click the device labeled IomegaEZ, and you will see the Iomega StorCenter Console for the Iomega device.
- **Mac** — Browse to your Iomega device through **Finder**, **Shared**, **All** and use **Go**, **Connect to Server** to connect to Shares on your Iomega device.

How do I ...

set up my Iomega device
install Iomega Storage Manager

Setup Page

The Setup page opens when you first access the Iomega StorCenter px12-400r from the Home Page or the Iomega Storage Manager. On this page, you can configure some basic device features by clicking the appropriate link. The current setting of the feature displays above the link. You can also configure all features shown on the Setup page by accessing the specific features directly.

Network Connection

Connecting the Iomega StorCenter px12-400r to Your Network

First, check the package contents.

Verify that the box contains the following items:

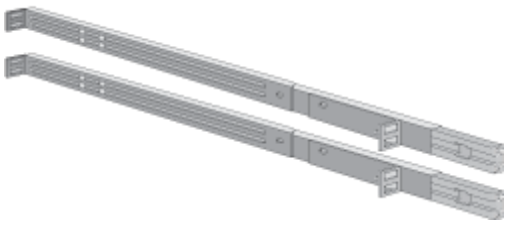
1. px12-400r (models may vary)

2. Quick Start Guide

3. Power Cables

4. Ethernet Cable

5. Rail kit (models may vary)



Connecting the px12-400r

Initial Setup

If you have purchased more than one px12-400r, complete all steps on one device before setting up additional devices.

1. Use the included network cable to connect the px12-400r to a network hub or switch.

2. Connect the included power cords to the power supply connectors on the back of the px12-400r and to an Uninterruptible Power Supply (UPS). This provides redundant power for your px12-400r.

3. Power on the px12-400r.

4. From a computer on your network, open a web browser and go to www.iomegasetup.com to set up your px12-400r on your network. For best results, use a computer that is connected to the same subnet or network segment as the px12-400r.

   NOTE: You can access the Iomega StorCenter px12-400r Console directly by entering the IP address or model name of your px12-400r in your computer's web browser. To use the model name on a Mac, add .local after the name in the browser (for example, px12-400r.local).

5. OPTIONAL: if desired, install the Iomega Storage Manager, QuikProtect, and Media Aggregation software.

   If you install Iomega Storage Manager, its icon will appear in the System Tray (Windows) or Menu Bar (Mac). The Iomega Storage Manager will automatically scan your network and connect to available Shares.

   If you receive a message from your operating system's firewall alerting you of network activity, be sure to unblock communications.

   Mac Users: Shares on the px12-400r will mount and appear on the Mac Desktop.

   PC Users: Shares on the px12-400r will automatically be assigned a drive letter and will be available in the Network Drives section under My Computer.

How do I ...

view information about my device components

Network Settings

The Network page of your px12-400r is where you make changes to set up network connectivity. The Network page displays your current network settings and enables those settings to be modified. On this page, you can identify your DNS servers and WINS servers and how your system's IP address is determined. Most system IP addresses and other network settings can normally be configured automatically.

Manually Configuring Your Network

If you are comfortable with network technology and want to configure the network, refer to Manually Configuring the Network.

Bonding NICs

If your px12-400r has multiple network interface cards (NICs), you can bond those NICs. Refer to Bonding NICs.

Enabling Jumbo Frames for Each NIC

You can enable jumbo frames for each NIC in your px12-400r by expanding the **Information** section for a NIC and selecting a jumbo frame size from the **Jumbo Frame** drop-down menu. Valid jumbo frame sizes are 4,000 or 9,000 bytes. If you do not want jumbo frame support, select **None** from the **Jumbo Frame** drop-down menu. Jumbo frame support is useful for transferring large files, such as multimedia files, over a network. Jumbo frame support increases transfer speed by placing large files in fewer data packets. It also reduces the demand on the device hardware by having the CPU process more data in fewer data packets.

Jumbo frame support should only be enabled if you are sure your network is jumbo-frame compatible and all network devices have been configured to support jumbo frames. It is recommended that you confirm all network interface cards (NICs) are configured to support jumbo frames before enabling this feature.

VLAN Settings

Each NIC in your px12-400r can be added to up to four Virtual LANs (VLAN). For more information on adding a NIC to a VLAN, refer to VLAN Settings.

Manually Configuring the Network

There are various settings in the network setup that you can manually configure.

1. Click **Modify network settings**.
2. Uncheck **Automatically configure DNS, WINS, and all IP addresses (DHCP)**.
3. **DNS Servers** — enter the IP addresses of the DNS (Domain Name System) servers. DNS is used for translating the domain name to IP addresses.
4. **WINS Servers** — enter the IP addresses of the WINS server.
5. From the **Bonding Mode** drop-down menu, choose one of the following:
    - **Transmission Load Balance** — increases bandwidth by distributing the load across multiple NICs.
    - **Link Aggregation** — increases bandwidth by distributing the load across multiple ports in a switch.
    - **Failover** — provides recovery from a failure, so if one NIC should fail, your system still has network connectivity with the other NIC.
6. Click **Apply** to save your settings.

    If a DHCP server is unavailable for a network interface card (NIC), the device could auto-assign an IP address, or you can uncheck the **Automatically acquire network address (DHCP)** checkbox found in the **Information** section of a NIC.
7. You can change the following settings in the **Information** section:
    - **IP Address** — the static IP address of the px12-400r. Use an available IP address in the range used by the LAN.
    - **Subnet Mask** — the subnet that the IP address belongs to. The default value is 255.255.255.0.
    - **Gateway** — enter the gateway IP address in this field.
8. Click **Apply** to save your settings.

VLAN Settings

Each NIC in your px12-400r can be added to up to four Virtual LANs (VLAN). For more information on adding a NIC to a VLAN, refer to VLAN Settings.

Bonding NICs

If your px12-400r has multiple network interface cards (NICs), you can bond those NICs. Refer to Bonding NICs.

Bonding NICs

Bonding network interface cards (NICs) is a way to provide redundancy for your px12-400r on the network. If one NIC should fail, your px12-400r will remain accessible on the network if that NIC is bonded to others. You can bond two or more network interface cards (NICs) in your px12-400r by selecting the NICs and clicking **Apply**.

Use the following procedure to bond NICs.

1. On the Network page, expand the NIC number and then expand the **Bond Network Interface** section.

2. Check the checkboxes next to the NICs that you want to bond to the selected NIC. For example, if you selected NIC 1, and your configuration includes four NICs, you could bond NIC 1 to NIC 2, 3, and/or 4.

3. Click **Apply** to save your settings.

   The section updates and displays the NICs that are bonded to the selected NIC.

Unbonding NICs

1. To unbond a NIC, uncheck the box next to the bonded NIC.

2. Click **Apply** to save your settings.

VLAN Settings

A VLAN (Virtual Local Area Network) is a network of devices that are joined into one broadcast domain, even if the devices are not physically connected to each other. VLANs are useful for creating smaller networks within a larger LAN; for example, a legal department in a company might be on its own VLAN because it has sensitive documents that only certain personnel should have access to. The smaller networks that VLANs create do not require any additional physical resources, such as additional cabling. Your Iomega StorCenter px12-400r can be configured to support VLANs.

VLAN is configured for each NIC, but it is not supported on bonded NICs. If a NIC is bonded, you must unbind it first to configure it for a VLAN.

Adding a VLAN

1. To add a VLAN, expand the **VLAN Settings** section of a NIC.
2. Click **Add VLAN**.
3. Enter a VLAN ID value between 2 and 4094. You can enter up to 4 VLAN IDs for each NIC. A VLAN can obtain its network settings from DHCP, or you can uncheck DHCP and enter the IP address, subnet mask, and gateway manually.
4. Refer to Network Settings Overview for information about jumbo frames.
5. Click **Apply** to save your changes.

Deleting a VLAN

In the **VLAN Settings** section click **Delete** to delete the VLAN.

Naming Your Iomega StorCenter px12-400r

You can provide a meaningful name for your px12-400r using the Device Identification page. This page in the Iomega StorCenter px12-400r Console enables you to change the Storage Device Name, the Storage Device Descriptive Name, and the Workgroup Name.

Change any of these by editing the text fields. Click **Apply** to save your changes.

Device Name

Enter a name for the Iomega device. Use a name that will help you identify it on your network.

Device Descriptive Name

Enter a descriptive name for the Iomega device device. This name can provide additional detail that identifies the device.

Workgroup Name

Enter a workgroup name for the Iomega device if you need to change the default name. The workgroup name identifies a group of computers that share information with each other. Change the workgroup name only if you explicitly define a workgroup on your network. Most users won't need to change the workgroup name, unless they have explicitly defined a different workgroup on their other computers.

How do I...

enable security

Configuring Your Iomega StorCenter px12-400r to Use Active Directory

If you have an existing Active Directory user organization, you can incorporate it into the Iomega StorCenter px12-400r Console.

Note: When you configure Active Directory, you enable security on your px12-400r.

---

1. To configure Active Directory, manually add the px12-400r to your DNS server. Set the px12-400r DNS setting to point to your DNS server. On the Network page, uncheck **Automatically configure all network settings**, type the IP address of your DNS Server in the text box, and click **Apply** to save your settings.

2. Configure the px12-400r to join the Active Directory domain. **Active Directory** — select Active Directory mode if you already have an existing user organization, such as Active Directory, that you want to incorporate into the px12-400r.

3. Provide the following connectivity information:

    - **Domain Name** — the actual name of your Active Directory domain, for example, sohoad.com.
    - **Domain Controller** — the actual name or IP address of your Active Directory Server, for example, ad-server.sohoad.com or 10.14.50.12.
    - **Organizational Unit** — an optional predefined subset of directory objects within an Active Directory domain.
    - **Administrator Username** — the Active Directory username with domain administrator privilege.
    - **Administrator Password** — the Active Directory password for the specified Active Directory username.
    - **Users/Groups Refresh Interval** — how often the px12-400r should refresh the list of available users and groups from the Active Directory server.
    - **Enable Trusted Domains** — enables your px12-400r to allow access to other domains.

4. Click **Apply** to save your settings.

Enabling Active Directory Trusted Domains

By enabling Active Directory trusted domains on your px12-400r, you enable the importing of users and groups from other trusted domains to your px12-400r device. Those users and groups from other domains will then have access to features on your px12-400r, including accessing folders and documents in Shares, and joining any Personal Cloud of which the device is a member.

Now that you have enabled access to all trusted domains, you can add users and groups from those trusted domains to your px12-400r. For more information, refer to Manage Users and Groups with Active Directory.

How do I ...

enable security

Obtaining Alerts About Your Iomega StorCenter px12-400r

You can configure your px12-400r to send email alerts when problems are detected. This is done through the email notification feature. Email notification provides a destination for emails sent by the px12-400r when problems are detected. To provide a destination email address, enter the following information:

- **Destination Email Addresses** — enter a valid email address or addresses. This email address provides a destination for messages sent by the px12-400r when problems are detected by the system. You can add multiple email addresses by separating them with commas, spaces or semicolons.
- Check **Send a test email message** to confirm that email notification is working properly.
- Check **Configure custom SMTP settings** only if your network blocks SMTP traffic, requiring additional credentials, such as a corporate firewall. Most users will not need to check this option. If checked, enter the following additional information to identify your SMTP server:
    -
    - **Email Server (SMTP)** — enter the address of your SMTP server.
    - **Sender Email Address** — enter an email address for the px12-400r to use as the *From* address when it creates messages.
    - **Email Login** — enter the username used to log into the email account you entered above.
    - **Email Password** — enter the password for the email account.
    - **Confirm Password** — confirm the password for the email account. It must match the password provided above.

Note: If your email application uses a SPAM blocker, it is recommended that you add a sender email address to your safe list. If you do not define additional credentials, the default sender email is: sohostorage@emc.com

Click **Apply** to save your changes.

Using Your Iomega StorCenter px12-400r in Various Time Zones

You can set the date and time used on your px12-400r , so that it can appear to be in one time zone, when it actually may be in a different one. This can help your users have the correct date and time if they live and work in a location different from your px12-400r . You can set the date, time, and time zone through the Date and Time feature.

Note: When an Active Directory Domain is in use, the storage device synchronizes time with the domain controller.

in a different one. This can help your users have the correct date and time if they live and work in a location different from your px12-400r. You can set the date, time, and time zone through the Date and Time feature.

Note: When an Active Directory Domain is in use, the storage device synchronizes time with the domain controller.

1. To change time zones, select a Time Zone from the drop-down menu, and then select how time will be set for the px12-400r:

Internet Time Server

By default, Automatically synchronize with an internet time server and Use the default time server are selected. To specify a time server, select Specify the time server and type the URL of the internet time server you wish to use in the text box that displays.

Manual

Select Manually set date and time. To set the current date and time, click the appropriate icon for calendar and clock settings.

2. Click **Apply** to save your changes.

Setting the Display Language for Your Iomega StorCenter px12-400r

You can set the display language for your px12-400r through the Languages page.

The language used by the Iomega StorCenter px12-400r Console is based on the preferences configured in your browser. You can change the language used in this program by modifying your browser's preferred language settings.

Click **Apply** to save your changes.

Printing Documents

Printing documents from your Iomega StorCenter px12-400r is simple after you have attached a compatible printer to the px12-400r. The Printers page displays a table of printers that are attached to the px12-400r. The table contains for each printer the name, model, status, and number of documents waiting.

To attach a printer, simply plug a supported printer's USB cable to a USB port on the px12-400r. Once attached, the printer will appear in the table. When the cable is unplugged, the printer will be removed from the table.

Setting up Personal Cloud, Security, and File Sharing

After you have configured some basic features of your Iomega StorCenter, you may also want to set up an Iomega Personal Cloud, security, or file sharing.

You can set up a Personal Cloud to allow invited users access to content on your Iomega StorCenter. This content can be in private Shares that are exclusive to the users who join the Personal Cloud, which adds an additional layer of security to your content. In addition, you may want to join other trusted devices to the Personal Cloud so that content on those devices can be made available to Personal Cloud users. For more information about Personal Clouds, refer to the Personal Cloud overview.

You can enable security so you can secure Shares, create users, and allow selected features to be enabled. When you create users, you limit access to your Iomega StorCenter to those specific people, and when you secure Shares, you limit data access to those specific users. For more information on security, refer to What Is Security and Do I Need It?

It is recommended to set up file sharing so that content can be added to your Iomega StorCenter, and that content can be made available in a wide variety of ways, including users of your Iomega StorCenter and content features such as Active Folders and media sharing. For more information, refer to the Sharing Overview.

How do I ...

create an Iomega Personal Cloud

set up security

set up file sharing

Sharing Files

Sharing Overview

Your Iomega StorCenter is set up for storing, retrieving, and accessing files among users, client computers, and applications.

Note: File sharing is accomplished by creating Shares; setting up security, which includes creating users; setting up media services; and configuring Active Folders.

Interfaces for Sharing

Your Iomega device has three separate interfaces for file sharing:

Iomega StorCenter Console

You manage the creation of Shares through the Iomega StorCenter Console.

Iomega Storage Manager

Optionally installed on your local computer, Iomega Storage Manager discovers any Iomega storage devices on your subnet, maps device Shares to computers, and provides local access to your content. It provides access to Shares through your computer's file management program, such as Windows Explorer or Mac Finder, allowing you to drag and drop many files between your computer and the Iomega device. Installing Iomega Storage Manager is optional.

Home Page

Serves as a web-accessible interface to your Iomega device. The Home page content is configured using the Iomega StorCenter Console. The Home Page displays any public Shares. It can also display secured Shares accessible only to users who log in to the Iomega device. You can access the Home page of your Iomega device by entering the device name or IP address directly in your browser. If security is enabled and you are an administrator user, you can access the Iomega StorCenter Console from the Home page by clicking .

How do I ...

create Shares
enable security
create users

Shares

What are Shares and How Do I Organize Content with Them?

Shares are folders that contain all types of content, including documents, pictures, and music files. Shares can be public, meaning anyone accessing your px12-400r can access the content in the Shares. Shares can also be secured, which means access to content in them is limited to a select group of users.

All Shares on an px12-400r are displayed on the Shares page. The Shares page displays a table that contains folders, connected drives, and any cloud storage to which your Iomega StorCenter px12-400r Console is connected. The Properties column displays the features that are enabled for each Share.

Share Information

The Information section displays the Share name, graphically displays the space usage of the Share, and allows you to view the content using the web-based content viewer.

To view the content of a Share, click **View Content** to open the Content Viewer.

To learn how to modify your Share information, refer to Managing Shares.

Access Permissions

The Access Permissions section contains a list of users who currently have access to that Share. Access Permissions displays when the px12-400r is secured, otherwise the section is not included in the Share. If "Everyone" has access to Shares that means your content can be viewed by anyone with access to your network without that person needing a username or password.

To learn how to modify Access Permissions on a Share, refer to Managing Shares.

Active Folders

Follow the link to the Active Folder options for information on configuring each:

- Email Distribution
- Facebook
- Flickr
- Photo Resize
- Torrents
- YouTube

How do I...

add a Share
manage a Share
delete a Share

Adding Shares

1. From the Iomega StorCenter Console, click **Shares**.
2. To add a new Share, click **Add a Share**. Type a name for the Share. All Shares must have a name. Names cannot exceed 32 characters. The following are not valid Share names: global, homes, printers.
3. Click **Create**. To modify an existing Share, click the Share row to expand the Share.

How do I ...

manage Shares
delete Shares

Managing Shares

You can change Share information, change access permissions, make a Share an Active Folder, use Share volumes, and modify a Share volume.

If available, you can also enable NFS secured access.

Changing Share Information

1. Modify the existing name for the Share.
2. Choose whether to enable media sharing. When Media sharing is enabled, the media server scans this Share for any media content and makes it available to anyone with access to your network, even if this Share is secured. If you do not want media content made available to anyone, do not check this option. When Media sharing search is enabled, displays in the Properties for that Share.
3. To view the content of a Share, click the **View Content** link to open the Content Viewer.
4. Click **Apply** to save your changes.

Changing Access Permissions

Note: You should enable security on your Iomega StorCenter before changing access permissions.

---

1. Expand **Access Permissions** to change user permissions to this Share. A security icon displays in Properties indicating a secure Share. When a secure Share is first created, Everyone has read and write access to that Share by default, which means that everyone on your network can read, write, and delete files to and from that Share. When user Everyone has Read and Write permissions to a Share, the Share is not secure and is open to all users.
2. Check **Allow users to change file level security** to allow file and folder permissions to be set through other programs, such as Windows Explorer, independent of the Iomega device. Setting this option allows users to put additional access restrictions on individual files and folders.
3. To limit access to this Share to a specific set of users, click **Add access permissions** and choose one or more users from the pop-up window. If you have created groups, you can also limit access for them in this way.
4. In the **Access Permissions** section, check Read, Write, or both to set access to this Share for each user. To remove a user, leave both Read and Write unchecked for that user. If you grant Read and Write permissions to Everyone, the list of users is also cleared since all users (Everyone) has access to this Share. If you have created groups, you can also limit access for them in this way.
5. Click **Apply** to save your changes.

Enabling NFS Secured Access

1. To enable NFS, first click the switch on from the Protocols page.
2. On the Shares page, select a secure Share and expand the NFS section. You cannot apply a rule to a public Share.
3. Click **Add an NFS rule** to add a **Host Name** for the rule. Rules are added to specify the hosts that are allowed to access Shares using NFS. Use this table to add NFS rules to specify access for hosts. For example, *.cs.foo.com matches all hosts in the domain cs.foo.com. To export a Share to all hosts on an IP address or local network simultaneously, specify an IP

address and netmask pair as address/netmask where the netmask can be in dotted-decimal format, or as a contiguous mask length. For example, either /255.255.252.0 or /22 will result in identical local networks.

4. When the rule is added, read access is automatically set to the Share. Select **Write** to allow users to write to that Share. Use and to modify the rule priority for NFS access.
5. Click **Apply** to save your changes.

Making a Share an Active Folder

1. You can optionally enable Active Folders on a Share to allow you to associate this Share with a specific feature that will happen automatically when files are copied to the Share. For example, you can enable a Share as a social media active folder to upload a file to a social media site. Refer to Sharing Content with Social Media Overview. You can only set one Active Folder option per Share.
2. Expand the **Active Folder** section and check **Enable**. Select one of the following Active Folder options and follow the link for details on configuring each:
    - Email Distribution
    - Facebook
    - Flickr
    - Photo Resize
    - Torrents
    - YouTube
3. Click **Apply** to save your changes.

Using Share Volumes

When you create a Share, you can use an existing volume or create a new one for that Share. After that Share is created, you cannot move it to a different volume. You can modify the volume by changing its size. You can also determine if the volume can automatically grow in size.

1. To set the volume for a Share as you are creating it, click **Change volume allocation** in the **Information** section.
2. Choose whether to use an existing volume or to create a new one. For more information on existing volumes, refer to Volume Management.
3. Select an existing Storage Pool in which to place the volume.
4. If you are selecting from more than one existing volume, select a volume from the **Volume** drop-down menu.
5. If you are creating a new volume, enter a name for the volume in the **Volume** text box.
6. Enter a size for the volume. You cannot reduce this size later.
7. Click **OK**.
8. In the Information section, click **Apply** to save your changes.

Modifying a Share Volume

1. Click **Change volume allocation** in the **Information** section.

2. Enter a new size for the volume.
3. Click **OK**.
4. In the Information section, click **Apply** to save your changes.

How do I ...

add a Share
delete a Share
share content with social media

Deleting Shares

To delete a Share:

1. From the Iomega StorCenter px12-400r Console, click **Shares**.
2. To delete an existing Share, click to expand the Share.
3. In the Information section, click **Delete** to delete the Share.
4. In the **Delete Share** confirmation pop-up window, click **Yes**.
5. If you do not wish to delete the Share, click **Cancel** to return to the Shares page.

How do I ...

add a Share
manage a Share

Using Protocols to Share Files

What Are Protocols and How Do I Use Them to Share Files?

Your Iomega StorCenter px12-400r uses communication protocols to mount file systems and allow files to be transferred between client computers and the Iomega StorCenter.

The px12-400r includes the following protocols for file sharing:

- AFP
- Bluetooth
- FTP
- TFTP
- NFS
- rsync
- SNMP
- WebDAV
- Windows DFS
- Windows File Sharing

AFP File Sharing for Macs

The Apple Filing Protocol (AFP) enables Apple file sharing, which is the preferred method for Mac users to access Shares. AFP is on by default.

To enable AFP, click the switch on.

Bluetooth File Sharing

Once a Bluetooth adapter is detected, files can be uploaded to a configurable destination Share on the px12-400r from a Bluetooth device.

Configuring Bluetooth settings

1. To enable Bluetooth, click the switch on.
2. Once Bluetooth Transfer is enabled, check the **Enable security** checkbox to require Bluetooth users to supply a unique PIN that they have defined before allowing them to transfer files to the destination Share on the px12-400r. If you have enabled security, you must define a unique PIN number, which will be supplied by devices attempting to upload data using Bluetooth.
3. To set the destination Share, click .
4. Click **Apply** to save your settings.

Note: To change any Bluetooth settings, click .

FTP File Sharing

On the Protocols page, click the switch to turn on FTP (File Transfer Protocol) and allow access to your Iomega StorCenter px12-400r.

Click to select either FTP or secure FTP (SFTP) or both. You must enable security to apply SFTP. If you select and enable SFTP, you cannot have the secure Rsync protocol enabled.

When you turn on FTP, you can send files to your px12-400r.

NFS File Sharing

On the Protocols page, click the switch to turn on NFS (Network File System) to allow remote hosts to mount file systems over a network and interact with them as though they were mounted locally to your Iomega StorCenter px12-400r.

Note: Select an option to choose how users on client computers are mapped to the px12-400r:

- To have all users, including root, map as guest, select **Treat client users as guest (all_squash)**. All files are owned by user guest, and all users accessing the px12-400r have the same access rights. If you have enabled Active Directory on your px12-400r, only this option is available for mapping client computers.
- To have all users map as themselves but root maps as guest, select **Allow full access for client users other than root (root_squash)**.
- To have all users map as themselves, including root, select **Allow all client users full access**.

Once enabled, add NFS access rules for each secure Share from the Managing Shares page. NFS provides another protocol for sharing storage data with Linux hosts. When NFS is enabled, you can configure rules for host-based access to secure Shares.

Rules can be added to secure Shares to specify the hosts that are allowed to access Shares using NFS. For example, *.cs.foo.com matches all hosts in the domain cs.foo.com. To export a Share to all hosts on an IP address or local network simultaneously, specify an IP address and netmask pair as address/netmask where the netmask can be in dotted-decimal format, or as a contiguous mask length. For example, either /255.255.252.0 or /22 will result in identical local networks.

To change any NFS settings, click .

---

rsync: Synchronizing Files with Another Storage Device or Other Computers

When you turn on this protocol, you can enable the Iomega StorCenter px12-400r as an rsync server. When the px12-400r is an rsync server, it can be used as a source and/or destination device for rsync Copy Jobs. Because of the fast and efficient nature of rsync, an rsync Copy Job can be faster than a Windows File Sharing Copy Job. For more information on Copy Jobs, refer to Copy Jobs.

If you enable the px12-400r as an rsync server, you can optionally set up a user account on the px12-400r for secure rsync Copy Jobs.

Configuring rsync server settings

1. To enable rsync server, click the switch on.
2. To create a secure user account, check **Configure secure rsync credentials**.
3. The username is preset as rsync. You can change this to a more meaningful user account name. Enter a password and confirm it for the rsync user account name. When you create a secure rsync user account on the px12-400r, you allow other devices to securely copy to or from it.
4. By default, rsync uses TCP port 873 for accepting requests. You can change this value to a different port number, if desired.
5. Click **Apply** to save your settings.

Note: To change any rsync server settings, click . You cannot enable rsync server if you have already enabled SFTP.

TFTP

On the Protocols page, click the switch to turn on TFTP (Trivial File Transfer Protocol) and allow access to your Iomega StorCenter. When you turn TFTP on, you can send files to your Iomega device using FTP.

Monitoring Your Device with an SNMP Management Tool

SNMP (Simple Network Management Protocol) provides information about the state of the Iomega StorCenter px12-400r to various management tools.

SNMP should be disabled unless you are specifically providing information to a management system that requires this information.

Configuring SNMP settings

1. To enable SNMP, click the switch on.
2. Enter a unique username and password to define the community.
3. Confirm your password.
4. Enter the IP address of the host in the **Trap Receivers** text box. To grant access to multiple receivers, list all of them in the text box, separating each entry with a space.
5. Click **Apply** to save your settings.

To change any SNMP settings, click .

WebDAV: Managing Files Using HTTP or HTTPS

WebDAV (Web-based Distributed Authoring and Versioning) is a protocol that provides web-based access to Shares on the Iomega StorCenter px12-400r. With WebDAV enabled on the px12-400r, you can view, add, or delete files through your WebDAV client using either HTTP for unencrypted access or HTTPS for encrypted access. HTTP offers faster performance, but is not secured. Access Shares using a URL such as http://devicename/WebDAV/Foldername. Refer to your operating system's documentation to learn how to access files through WebDAV.

Note: If your px12-400r has a remote access password, you must enter that password and the username *webdav* to access your device. Your px12-400r has a remote access password only if the device is not secured and a Personal Cloud was created on it.

Configuring WebDAV settings

1. To enable WebDAV, click the switch on.
2. To enable WebDAV for HTTP, check **Enable WebDAV Over HTTP**.
3. To enable WebDAV for HTTPS, check **Enable WebDAV Over HTTPS**.
4. Click **Apply** to save your settings.

Windows DFS: Creating a Distributed Windows File System

Windows DFS (Distributed File System) organizes Shares and files on a network, such that they appear to be all in one directory tree on a single px12-400r, even if the Shares reside on many devices.

Windows DFS terms

There are several terms to understand with Windows DFS.

Namespace

A virtual Share containing other folders that are located on different devices throughout a network.

DFS root

An object that consolidates all the folders in your network and makes them available through a single entry point. An example of a DFS root is \\ DeviceName\DFSRootName.

DFS link

A folder under the DFS root.

Configuring Windows DFS settings

1. To enable Windows DFS, click the switch on.
2. Enter a DFS root name. The DFS root name is the starting point of a DFS namespace.

   After entering a DFS root name, you add DFS links, which map to folders on other devices.

3. Click **Click to add a DFS link target** to begin adding DFS links.
4. Enter the DFS link name, which includes the name of the host and Share to which you are linking.
5. Click **Apply** to save your settings, or click **Cancel** to discard your changes.

Windows File Sharing

Windows File Sharing allows you to work in Workgroup mode, using Iomega StorCenter px12-400r Console to create users and manage access. To enable Windows File Sharing, click the switch on.

Sharing Content through the Home Page

Sharing Your Content with the World

When you set up the Home Page of your Iomega StorCenter px12-400r, you are presenting public content to anyone who accesses your px12-400r. That public content includes a slideshow and public Shares.

You can manage the look of the Home Page by using the Home Page Settings page. This page allows you to display the slideshow, display public Shares, name the Home Page, and turn the Home Page on or off.

1. From the Iomega StorCenter px12-400r Console, click **Home Page Settings**.
2. Click the slider switch to On to enable the Home Page on your px12-400r.
3. Enter a title for the Home Page. This title displays in the top banner of the Home Page when users access the px12-400r.
4. Check **Display Shares** to display public Shares. When you select to display Shares, the user sees all public Shares on the px12-400r.
5. Check **Display slideshows** to display picture slideshows that are in folders on the px12-400r. Click **Manage slideshows** to configure any slideshows you want to display. The slideshow location can be any folder attached to the px12-400r, including a USB drive or DFS location.
6. Click **Apply** to save your changes, or click **Cancel** to discard your changes.

Deleting a Slideshow

To delete a slideshow from the list of available slideshows, click . After you delete a slideshow, you can configure a different one.

How do I...

create Shares

add custom home page content

Adding a Custom Home Page

You can customize the look of the home page of your Iomega StorCenter px12-400r to include html pages and client-side scripting, such as Javascript. This customized home page replaces the default home page on the px12-400r. In addition, there are applications available on www.lifelineapps.com that can enhance your home page content.

You add your custom html content to a Share on your px12-400r and then specify its location on the Home Page Settings page.

Applying the Customized Home Page

1. Click the **Home Page Settings** feature from the Iomega StorCenter px12-400r Console.
2. On the Home Page Settings page, select **Customized home page settings**.
3. In the Home Page Name field, enter the name of the start page of your custom home page. By default, the name is index.html.
4. Specify the destination Share where the start page and your html content exists on your px12-400r by clicking and navigating to the Share.

   Note: You cannnot access the destination Share through the WebDAV interface. Access through WebDAV is permanently disabled.

5. Select the Share name and click **Apply**.
6. Click **Apply** to save your settings.

Automatically Sending Content to Multiple People at Once

You can send content to multiple people at once using an email distribution active folder. You can configure a Share as an Email Active Folder so that when you add files to that Share, they are automatically sent to the recipients on the email distribution list. To configure a Share as an Email Active Folder, access Shares from the Iomega StorCenter px12-400r Console, select or create a Share, and expand the Active Folders section to enable and configure email distribution.

How to Set Up an Email Distribution Active Folder

Note: Email Distribution lets you email your files to friends and family right from your Iomega StorCenter px12-400r Console. Use Email Distribution to share files with an email list.

Note: To prevent email distribution list spamming, the px12-400r allows lists of 250 or fewer email recipients and sends a maximum of six emails in a 24-hour period.

Refer to Managing Shares for more information on managing Shares and Active Folders.

Configuring an Email Distribution Active Folder

1. From the Iomega StorCenter px12-400r Console, click **Shares**.
2. Select a Share to use as an Email Distribution Active Folder, and click to expand the Active Folder section.
3. Check **Enable**.
4. Select **Email Distribution** from the drop-down menu.
5. Include an email address in the **Sender Email Address** text box. Distribution is sent from this email address.
6. You can add multiple email addresses in the **Email To:** text box by separating them with commas, spaces, or semicolons.
7. Add a subject and email message for your recipients.
8. Check **Send the file as an attachment**, **Send a link to the file**, or both.
9. Click **Apply** to save your changes.
10. Once configured, all files in this Share are sent by email to your recipients. Click **View Transfer History** to see the transfer activity from this Share to your account.

How do I...

manage a Share

Sharing Content Using Social Media: Overview

If you have an account with social media services such as Facebook, Flickr, or YouTube, you can share content on your Iomega StorCenter px12-400r with your friends and family using one or more of these social media sites. To share your content using social media sites, create Shares called Active Folders, and connect each Active Folder with a social media account. Refer to the help topic links below for more information on these procedures. When you add photos and movies to an Active Folder, those files are automatically uploaded to the social media site associated with that Active Folder. If you have photos or movies you want to share with others, this is a great way to make your content available to people who may not have access to your px12-400r.

If you have configured a Personal Cloud on your px12-400r, you can grant Personal Cloud users access to Shares and Active Folders. This is useful if you want to allow users to add files to your social media sites. For example, if your px12-400r has a Flickr Active Folder, you can grant Personal Cloud users access to that Active Folder. In this manner, when photos are added to the Flickr Active Folder, either by you or by Personal Cloud users, those photos are uploaded automatically to your Flickr account.

Note that an Active Folder can only be associated with one social media account. For example, if you want Active Folders for your Facebook and YouTube accounts, create two Active Folders, and assign one Active Folder to Facebook, and one to YouTube. Using this example, any photos you add to your Facebook Active Folder are automatically uploaded to your Facebook page, and any movies you add to your YouTube Active Folder are automatically uploaded to your YouTube page. Not only is this a fast and easy way to share content, but uploading content to your social media sites provides an additional backup of your content, as the content is stored both on your px12-400r and at your social media accounts.

How do I...

make a Share an Active Folder
upload to Facebook
upload to Flickr
upload to YouTube

Managing Your Content

You manage content on your Iomega StorCenter px12-400r using the Content Viewer. The Content Viewer is a graphical file browser that lets you view and manage content in the Shares on your px12-400r.

The Content Viewer is divided into two panes. The left pane lists the Shares on the px12-400r and allows you to delete or add a Share. If you select a Share that contains pictures, you can start a slideshow of the pictures in that Share. The right pane lists the files and folders in a Share and allows you to delete content or upload a file to the Share.

To delete multiple files simultaneously, hold the Ctrl key on your keyboard and select each file, or drag your mouse over the filenames. Share content can be sorted, and you can switch between a list view and a thumbnail view of the files. When you are looking at content in a list view and you hover your mouse over an image, a thumbnail view of the image displays next to your mouse. If all the content cannot fit on one page, there are pagination controls that allow you to continue browsing the content.

Transferring Content to and from Your Iomega StorCenter px12-400r with Copy Jobs

You can transfer content to and from your px12-400r using the Copy Jobs feature. Copy Jobs copies files from one storage device to another, either by a set schedule or immediately by the user. An example of a Copy Job scenario is if you keep pictures from your digital camera on a separate USB drive, but you also want to maintain a backup of these pictures on your px12-400r. Using Copy Jobs, you can create a task that copies your photos on the USB drive to a Share on your px12-400r, and you can set that task to a schedule so the images automatically copy at a specific time. This ensures that your photos are always safely backed up to your px12-400r in the event your USB device ever fails or is lost.

Note: While a Copy Job copies all data from one NAS device to another, it does not copy permissions or access rights from one NAS device to another.

All saved Copy Jobs display on the Copy Jobs page. From there, you can manually start and stop a Copy Job, view Copy Job information, modify a Copy Job, check its last run status, and, if applicable, view when the Copy Job is next scheduled to run.

When defining a Copy Job, you can copy data from or to any of the following:

- Any NAS device automatically discovered on the same subnet as your px12-400r
- Any NAS device that you manually add to the subnet using the Iomega Storage Manager
- Any external storage device, such as a USB device, connected to your px12-400r
- A Windows computer that is automatically discovered on the same subnet as your px12-400r

When selecting what data to copy on the source storage device, you can choose a specific folder or all folders. You can also copy from a folder on an external storage device mounted to your px12-400r.

When selecting the destination device, you can copy files to the top-level folder on the destination device (the default option), or to an existing folder on this device, which adds the copied files into folders.

You can manually start or stop a Copy Job by clicking start or stop buttons on the Copy Jobs page. You can schedule a Copy Job to run automatically at a set day and time.

Copy Jobs Limitations

- Copy Jobs does not establish a continuous replication or mirroring relationship between the source and destination devices. You should not set up Copy Jobs for disaster recovery.
- Copy Jobs does not support transferring content from iSCSI drives.

Getting Content from a USB External Storage Device

You can transfer content to your Iomega StorCenter px12-400r from external USB storage devices. The External Storage page displays a list of externally connected storage devices. You can connect supported external storage to your px12-400r using one of the provided USB ports. When you connect external storage to your px12-400r, that device content is accessible from the **Shares** page.

Safely removing external storage

Click to safely remove the external storage. A confirmation dialog will display. Click **Yes** to remove the external storage. When the external storage has been removed from the **External Storage** table, it is safe to remove, and you may unplug it from the px12-400r. When the external storage is safely removed, its associated Share is removed as well.

iSCSI: Creating IP-Based Storage Area Networks (SAN)

iSCSI Overview

The iSCSI page allows you to create iSCSI drives on your Iomega StorCenter px12-400r and allows the Iomega Storage Manager to communicate with those drives over a network. An iSCSI drive provides a single place for all your storage, which you can divide as needed to support all computers in your enterprise business. iSCSI is useful for transmitting large blocks of data over a network at a high speed.

Only one client computer can connect to an iSCSI drive at a time, so iSCSI drives are not for shared data. If your business is clustering clients, then a cluster can access iSCSI drives.

How do I ...

add an iSCSI drive
manage an iSCSI drive
delete an iSCSI drive

Adding iSCSI Drives

To add an iSCSI drive:

1. From the Iomega StorCenter Console , click **iSCSI**.
2. When the iSCSI page opens, click **Add an iSCSI drive**.
3. If your Iomega device has multiple Storage Pools, select the desired Storage Pool from the drop-down menu.
4. Enter a name for the iSCSI drive. How you name your iSCSI drive will depend on your Iomega StorCenter meeting one of the following conditions:
    - If the **iSCSI/Volume Name** field displays by itself, enter a name for both. This field displays when your Iomega device is new, has no existing volumes, and supports multiple volumes.
    - If the **Name** field displays by itself, enter a name for the iSCSI drive. This field displays when your Iomega device is new or being upgraded and has only one volume.
    - If the options **Create a volume** and **Use an existing volume** display, select:
        - **Create a volume** to create a new volume for your iSCSI drive. This option displays when your Iomega device is new, or if you are upgrading your Iomega device and it has available space in its Storage Pools.
        - **Use an existing volume** to use an existing empty or shared volume. This option displays when you are upgrading your Iomega device, have available space in your Storage Pools, and have already created multiple volumes. To use an existing empty volume, select **iSCSI/Volume Name** and enter a name for the iSCSI drive and volume. To use an existing shared volume, select **Shared Volume**, select the existing volume, and enter a name for the iSCSI drive.
5. Enter a size for the iSCSI drive. The size must be smaller than the free space available on your Iomega device.
6. Click **Create** to create the iSCSI drive.

Enabling iSCSI Drives

1. Click **Settings** to begin configuring an iSCSI drive.
2. To set the discovery of the iSCSI drive using iSNS, check **Enable discovery with iSNS**.
3. Choose one of the following options:
    - **Use local iSNS server** — the device acts as an iSNS server for the iSCSI drives.
    - **Use external iSNS server** — you supply the IP address or host name of the external iSNS server for the iSCSI drives.
4. To enable the Challenge Handshake Authentication Protocol (CHAP), check **Enable two-way authentication (Mutual CHAP)**. With Mutual CHAP enabled, the client performs an additional check to confirm that it is using the correct device.
5. Enter a device secret (password) for Device Secret and then enter it again in the confirm box.
6. Click **Apply** to save your changes.

Connecting to iSCSI Drives

You can connect iSCSI drives on your Iomega StorCenter to your computer using Iomega Storage Manager or the Microsoft software initiator. If you are using another type of software or hardware initiator, you must use the native tools provided with your initiator to connect your iSCSI drives.

Caution: Attempting to connect two clients (iSCSI initiators) to the same iSCSI drive at the same time may result in data corruption or drive damage. The Iomega StorCenter Console prevents you from connecting two clients (iSCSI initiators) to the same iSCSI drive at the same time, but if you connect to an iSCSI drive using native tools, you may encounter this issue. You can use the **Connected Clients** section to view a list of client computers connected to your Iomega StorCenter that are running iSCSI initiator software. On the iSCSI page, expand an iSCSI drive, then expand the Connected Clients section. If the iSCSI drive is in use, you will see a list of connected client computers running initiator software.

How do I ...

manage iSCSI drives
delete iSCSI drives

Managing iSCSI Drives

The page describes how to:

- Assign iSCSI Drives to Volumes
- Change Access Permissions

Creating iSCSI Drives and Adding Them to Volumes

Every iSCSI drive that you create is added to a volume. In most cases, an iSCSI drive is automatically added to a volume when you create the iSCSI drive. In other cases, you may have to select some options to add your iSCSI drive to the appropriate volume.

On a new system where there are no existing volumes, a volume is created simultaneously when you create an iSCSI drive, and the iSCSI drive is assigned to that volume. On a new system where there are existing volumes, you can choose to assign the iSCSI drive to an existing volume or create a new volume and assign the iSCSI drive to that volume. For more information on existing volumes, refer to Managing Volumes.

On a system where there is only one Storage Pool and one volume, which can occur when upgrading from a previous version or device, you cannot assign an iSCSI drive to a volume.

If you are upgrading a system and it has only one volume, you cannot assign an iSCSI drive to a different volume. If you are upgrading a system and it has multiple volumes, you can assign an iSCSI drive to a new or existing volume.

Note: Unlike Shares, iSCSI drives cannot grow automatically. You must resize them manually.

Changing Access Permissions

1. Expand **Access Permissions** to change user permissions on an iSCSI drive. When an iSCSI drive is first created, the user Everyone has read and write access to that iSCSI drive by default, which means that everyone on your network can read, write, and delete files to and from that iSCSI drive.
2. To limit access to this iSCSI drive to a specific set of users, click the and choose one or more users from the pop-up window.
3. In the **Access Permissions** section, check **Read**, **Write**, or both to set access to the iSCSI drive for each user. If you create groups, you can also set access for groups in this way. To remove a user, leave both Read and Write unchecked for that user. If you grant read and write permissions to Everyone, the list of users is automatically cleared because all users (Everyone) have access to this iSCSI drive.
4. Click **Apply** to save your changes.

How do I...

add an iSCSI drive
delete an iSCSI Drive

Deleting iSCSI Drives

To delete an iSCSI drive:

1. From the Iomega StorCenter px12-400r Console, click **iSCSI**.
2. Click the iSCSI name to expand the iSCSI drive.
3. In the iSCSI Information section, click **Delete** to delete the iSCSI drive.
4. Click **Yes** in the confirmation pop-up window.
5. If you do not wish to delete the iSCSI drive, click **Cancel** to return to the iSCSI page.

Storage Pool Management

Understanding How Your Content Is Stored

Content on your Iomega StorCenter is stored in Shares. To access content in Shares, your client computer uses protocols, such as AFP and Windows File Sharing. Block-level data is stored in iSCSI drives. File systems maintain the physical location of content that resides in Shares. File systems in turn reside on volumes. iSCSI drives reside on volumes. Volumes allow you to partition space in Storage Pools, and you can use that space for file systems. Space in Storage Pools is also available for iSCSI drives. Storage Pools group physical drives together. All the drives in a Storage Pool should be the same size and all have the same protection, such as RAID 5.

Storage Pools

A Storage Pool is a grouping of drives with a certain storage size and an assigned data protection. A Storage Pool has a minimum of one drive. By default, your Iomega device has one Storage Pool.

Storage Pool Data Protection

For each Storage Pool, you can select its type of protection. Protection type determines how data is replicated across a Storage Pool and determines the amount of space used for data protection and storage. The drives in your Iomega device are protected using a built-in, pre-configured technology that redundantly stores data across the drives, so that if a single drive fails, in most cases, you will not lose any data. This technology, known as RAID (Redundant Array of Independent Disks), enables a series of drives to act together as a single storage system. If you create multiple Storage Pools, you can assign different RAID types to each Storage Pool.

For more information on selecting RAID types, refer to Changing RAID Protection Types.

Volumes

A Volume is a single storage area. A volume can be comprised of one or more hard drives. In a single-volume system, the volume consists of the entire storage space. Shares reside in volumes. iSCSI drives also reside in volumes.

How do I ...

add and manage Storage Pools
add and manage volumes
delete a Storage Pool
change RAID protection types
add or replace a drive

Adding and Managing Storage Pools

A Storage Pool is a grouping of drives with a certain storage size and an assigned data protection. A Storage Pool has a minimum of one drive. By default, your Iomega StorCenter px12-400r has one Storage Pool.

Cache Pools

When you create a Storage Pool, you can choose to create a cache pool. Cache pools consist of solid-state drives only, and they are intended to increase the performance of read and write operations.

To add a Storage Pool

1. On the **Drive Management** page, click **Add Storage Pool**.
2. In the **Information** section, enter a name for the Storage Pool.
3. To set the RAID protection, choose a value from the drop-down menu:

None (RAID 0)

Uses all of the storage space for data. Does not protect against data loss in the event of drive failure.

Mirror Stripe (RAID 10)

Uses half of the storage space for protection, leaving half for actual data. Protects data in the event of a single drive failure.

Parity (RAID 5)

Uses 1/4 of the storage space for protection, leaving 3/4 for actual data.

Double Parity (RAID 6)

Combines four or more drives in a way that protects data against loss of any two drives.

4. Select the checkbox of the drive or drives you want to add to the Storage Pool. All drives in a Storage Pool must be the same size.
5. Check **Enable periodic consistency check** to enable a monthly parity or mirror consistency check.
6. If commonly used Shares, Backups, Documents, Movies, Music, Pictures, and SharedMedia do not already exist on the px12-400r, check **Create commonly used Shares** to create these Shares and add them to the Storage Pool. This option is not available if you are creating a cache pool.
7. Check **Use for SSD Cache** to allow one or more solid-state drives (SSD) to be used as a cache pool. You can only designate SSDs as cache pool drives if they have not already been assigned to an existing Storage Pool. This cache pool becomes assigned to the Storage Pool you are creating.
8. Click **Create** to add the new Storage Pool.
9. Click **Cancel** to discard any changes.

Managing Drives

The Drive Management page provides settings for managing storage and lets you apply global settings

The Drive Management page provides settings for managing storage and lets you apply global settings for drives on your Iomega StorCenter px12-400r .

Setting Write Caching

Select a value for disk write caching.

Write caching is a mechanism that attempts to separate the fast processing speed of the px12-400r from the relatively slow mechanics of actually writing data to drive.

With write caching disabled, every write to drive causes the px12-400r to wait while the data is written to drive, which can slow performance. When write caching is enabled and the px12-400r sends a write request to the drive, it writes the data to cache (which is much faster) and sends an immediate acknowledgement to the px12-400r saying the write is complete. The system proceeds without waiting for the data to actually get written to drive, which occurs in the background.

While write caching does improve performance, there are some risks. The system responds that the data is written to drive when in fact it has only been written to cache. Should the px12-400r lose power, any data not completely written to drive is lost forever.

This is because cache memory is volatile. If you lose power, the contents of the cache are lost. Therefore, if there were any pending writes in the cache that were not written to the drive, they will be lost forever. Using a UPS (Uninterrupted Power Supply) can mitigate the risk associated with write caching, which is why it is recommended to only enable this feature when a UPS is connected.

Applying Global Drive Management Settings

Setting Write Caching

Select a value for disk write caching.

Write caching is a mechanism that attempts to separate the fast processing speed of the px12-400r from the relatively slow mechanics of actually writing data to drive.

With write caching disabled, every write to drive causes the px12-400r to wait while the data is written to drive, which can slow performance. When write caching is enabled and the px12-400r sends a write request to the drive, it writes the data to cache (which is much faster) and sends an immediate acknowledgement to the px12-400r saying the write is complete. The system proceeds without waiting for the data to actually get written to drive, which occurs in the background.

While write caching does improve performance, there are some risks. The system responds that the data is written to drive when in fact it has only been written to cache. Should the px12-400r lose power, any data not completely written to drive is lost forever.

This is because cache memory is volatile. If you lose power, the contents of the cache are lost. Therefore, if there were any pending writes in the cache that were not written to the drive, they will be lost forever. Using a UPS (Uninterrupted Power Supply) can mitigate the risk associated with write caching, which is why it is recommended to only enable this feature when a UPS is connected.

Applying Global Drive Management Settings

1. Click **Settings**.
2. Check **Add drives to storage system** to add a newly installed drive. You see this option only if there is at least one unused drive on the px12-400r.
3. To change the protection, choose a value from the drop-down menu:

Mirror (RAID 10)

Uses half of the storage space for protection, leaving half for actual data.

Parity (RAID 5)

Uses 1/4 of the storage space for protection, leaving 3/4 for actual data.

Double Parity (RAID 6)

Combines six or more drives in a way that protects data against loss of any two drives.

Striped (RAID 0)

Distributes data across several drives in a way that gives improved speed at any given instant.

None

Turns off data protection and leaves your data vulnerable to data loss.

4. Select a value for disk write caching.
5. Check **Enable periodic consistency check** to enable a monthly parity or mirror consistency check. The check helps to prevent a single drive failure from becoming a two-drive failure, resulting in data loss. The check runs for several hours and can affect performance of the px12-400r . If you do not want to run the check, uncheck this option.
6. Check **Use available drives as hot spares** to allow unused drives to become part of a RAID-protected storage pool. If a drive in a Storage Pool fails, all the data on that drive can be mirrored to the hot spare drive.
7. Click **Apply** to save your changes.

The Drive Management page displays a table that provides the following information about existing Storage Pools.

- **Name** — The name of the Storage Pool.
- **Protection** — The type of protection assigned to the Storage Pool.
- **Capacity** — The total amount of storage in the Storage Pool.
- **Used/Available** — Used is the space allocated to Shares. It is also space allocated to iSCSI drives. Available is the difference between capacity and used.

Drive status

An image on the Drive Management page provides information on the drive status of your px12-400r. The image displays the physical layout of drives and the drive slot numbers. If a drive has a circled letter, it is a member of a Storage Pool. If you hover your mouse over a drive in the image, the

ToolTip displays the drive model, size, and status, including if the drive is failing. If you hover your mouse on either a Storage Pool name in the table or on a drive in the Storage Pool image, all drives in the Storage Pool are highlighted.

How do I...

add Storage Pools
modify Storage Pools
delete Storage Pools
learn more about how content is stored

Modifying a Storage Pool

1. On the **Drive Management** page, expand the **Information** section of the Storage Pool you want to modify.
2. Enter a new name for the Storage Pool.
3. To change the protection, choose a value from the drop-down menu. You can change the protection of the following types of Storage Pools without having to recreate the Storage Pool and risk loss of data:
    - A 2-drive RAID 10 Storage Pool can change to a RAID 5 Storage Pool with three or more drives.
    - A RAID 5 Storage Pool can change to a RAID 6 Storage Pool, provided there are six or more drives in the existing RAID 5 pool. You can add drives to a RAID 5 or RAID 6 Storage Pool without recreating it.

      You cannot add drives to a linear or Raid 10 storage pool without recreating it.
4. Check **Enable periodic consistency check** to enable a monthly parity or mirror consistency check.
5. Select the checkbox of the drive you want to add to the pool. All drives in a pool must be the same size. You cannot remove any drives from the pool.
6. Click **Apply** to save changes to the Storage Pool.

Adding and Managing Volumes

A volume is a single accessible storage area with an allocated size. You can create volumes after creating Storage Pools.

Shares in Volumes

All Shares on the Iomega StorCenter px12-400r are added to volumes, and the size of the Share is limited by the free space of the volume. When you create a Share, you can add it to a volume at the same time. This is the simplest method for adding a Share to a volume. For more information on adding Shares to volumes, refer to Managing Shares. All iSCSI drives on the px12-400r are added to volumes, and the size of the iSCSI drive is limited by the free space of the volume. When you create an iSCSI drive, you can add it to a volume at the same time. This is the simplest method for creating iSCSI drives. For more information on adding iSCSI drives, refer to Managing iSCSI Drives.

To add a new volume:

1. On the **Drive Management** page, expand a Storage Pool, expand the **Volumes** section, and click **Add a Volume**.
2. In the **Information** section, enter a name for the volume in the **Volume** field.
3. In the **Size (GB)** field, enter a size in gigabytes (GB) for the volume. Note that both the allocated and available space for the volume displays. When you create a new volume, you can optionally enable encryption to protect your data if your px12-400r is lost or stolen. You can only enable encryption when you create a volume. Enabling encryption can reduce performance since information transferred to and from the drives must be processed using the 256-bit Advanced Encryption Standard (AES) protocol. To apply encryption to a volume, click the **Enable encryption checkbox.** There are two options for encryption: allowing the system to generate a passphrase, or creating one yourself. The passphrase is not a 256-bit encryption key.
    - **Generate and save passphrase on the system** — Select this option to allow the system to store a passphrase for the volume. This type of encryption works only when the px12-400r is powered down. If any drives are removed while your system is powered down, data on the encrypted volume will not be accessible. When the px12-400r is rebooted, the system-generated passphrase is automatically applied to the encrypted volume, unlocking it and enabling data access.
    - **Enter a passphrase** — This is a more secure type of encryption and is the recommended option. Click the **Enter a passphrase** option; then enter and verify a passphrase for the volume. You can change the passphrase at any time. After restarting the px12-400r , an encrypted volume is unavailable until you re-enter the passphrase. Note that the passphrase must consist of eight or more characters.

    After you create a passphrase, a new section for the volume appears called **Volume Encryption**. When you want to unlock a volume, enter the passphrase in this section.

    Note: It is recommended that you save a backup of the master key file in a secure location, separate from your px12-400r . You should not save the backup master key to a drive that is connected to your px12-400r . If a system failure occurs, the passphrase stored on your px12-400r may be lost, and your backup master key file is required to recover and access your data. Also, if you forget your passphrase, you can reset it using the backed-up master key. Click **Back up master key** to back up the master key file. To reset the passphrase, click **Reset passphrase with master key**, then enter a new passphrase and verify it.

4. To allow the volume to increase in size as needed, check **Grow automatically when needed** and enter a maximum size in the **Maximum Size** text box.

5. Click **Create** to save your changes.
6. Click **Cancel** to discard any changes.

Deleting a Storage Pool

1. On the **Drive Management** page, expand the **Information** section of the Storage Pool you want to delete.
2. Click **Delete**.

   The **Delete Storage Pool** window displays.
3. Select **Check this box if you want to delete the Storage Pools**.
4. Click **Yes** to delete the Storage Pool.
5. Click **No** to cancel the operation and retain the Storage Pool.

Note: Deleting a Storage Pool deletes all Shares and data contained within the Storage Pool.

Changing RAID Protection Types

You can change the RAID protection of existing Storage Pools. Before you can change RAID data protection of a Storage Pool, you must delete all data on the Storage Pool. If you are unfamiliar with RAID protection, it is recommended that you do not change this setting. You can also set the RAID protection type when you add drives to your Iomega StorCenter and create new Storage Pools.

To change the RAID type, expand the Information section of a Storage Pool on the Drive Management page, and choose a value from the Protection drop-down menu:

- Mirror Stripe (RAID 10)
- Parity (RAID 5)

For additional explanation on these RAID types, refer to Adding a Storage Pool.

Note that the displayed available capacity changes as you select different RAID types from the Protection drop-down menu. RAID array capacity is based on drive use, which differs for some RAID types.

Click **Apply** to change the RAID protection.

Click **Cancel** to retain your previous RAID configuration.

How do I ...

add and manage Storage Pools
add and manage volumes
delete a Storage Pool
add or replace a drive

Adding New Drives to Your Iomega StorCenter px12-400r

To install new hard drives in your px12-400r:

1. Before installing a new hard drive in your px12-400r, check the hard drive compatibility list online at www.iomega.com/support for approved and supported hard drive brands and models.
2. Mount the drive carrier containing the new drive in an available slot.
3. A confirmation dialog box displays as soon as the px12-400r detects the new hard drive. Click **Yes** to proceed.

   Note: All data on the drive is deleted.

4. You are re-directed to the Iomega StorCenter px12-400r Console.
5. Access the **Drive Management** page.

   Your px12-400r displays the new hard drives in the bays they are mounted in.
6. To create a RAID Array, you must install a minimum of two hard drives. The same confirmation dialog box displays. Click **Yes** to proceed.

   Note: You can create a Storage Pool using one hard drive if desired. You will not have any RAID protection options and can only select **None** from the RAID dropdown list while configuring your Storage Pool.

7. When all new drives are detected, click **Add a Storage Pool**.
8. Complete the Storage Pool configuration options and select the desired drives on which to build the Storage Pool by checking the boxes next to them. All drives in a Storage Pool must be the same model, manufacturer, and capacity.
9. Allow a few minutes for the RAID array and Storage Pool to build. When complete, the Storage Pool status displays on the Drive Management page.

Drive Management

Managing Drives

The Drive Management page provides settings for managing storage and lets you apply global settings

The Drive Management page provides settings for managing storage and lets you apply global settings for drives on your Iomega StorCenter px12-400r .

Setting Write Caching

Select a value for disk write caching.

Write caching is a mechanism that attempts to separate the fast processing speed of the px12-400r from the relatively slow mechanics of actually writing data to drive.

With write caching disabled, every write to drive causes the px12-400r to wait while the data is written to drive, which can slow performance. When write caching is enabled and the px12-400r sends a write request to the drive, it writes the data to cache (which is much faster) and sends an immediate acknowledgement to the px12-400r saying the write is complete. The system proceeds without waiting for the data to actually get written to drive, which occurs in the background.

While write caching does improve performance, there are some risks. The system responds that the data is written to drive when in fact it has only been written to cache. Should the px12-400r lose power, any data not completely written to drive is lost forever.

This is because cache memory is volatile. If you lose power, the contents of the cache are lost. Therefore, if there were any pending writes in the cache that were not written to the drive, they will be lost forever. Using a UPS (Uninterrupted Power Supply) can mitigate the risk associated with write caching, which is why it is recommended to only enable this feature when a UPS is connected.

Applying Global Drive Management Settings

Setting Write Caching

Select a value for disk write caching.

Write caching is a mechanism that attempts to separate the fast processing speed of the px12-400r from the relatively slow mechanics of actually writing data to drive.

With write caching disabled, every write to drive causes the px12-400r to wait while the data is written to drive, which can slow performance. When write caching is enabled and the px12-400r sends a write request to the drive, it writes the data to cache (which is much faster) and sends an immediate acknowledgement to the px12-400r saying the write is complete. The system proceeds without waiting for the data to actually get written to drive, which occurs in the background.

While write caching does improve performance, there are some risks. The system responds that the data is written to drive when in fact it has only been written to cache. Should the px12-400r lose power, any data not completely written to drive is lost forever.

This is because cache memory is volatile. If you lose power, the contents of the cache are lost. Therefore, if there were any pending writes in the cache that were not written to the drive, they will be lost forever. Using a UPS (Uninterrupted Power Supply) can mitigate the risk associated with write caching, which is why it is recommended to only enable this feature when a UPS is connected.

Applying Global Drive Management Settings

1. Click **Settings**.
2. Check **Add drives to storage system** to add a newly installed drive. You see this option only if there is at least one unused drive on the px12-400r.
3. To change the protection, choose a value from the drop-down menu:

Mirror (RAID 10)

Uses half of the storage space for protection, leaving half for actual data.

Parity (RAID 5)

Uses 1/4 of the storage space for protection, leaving 3/4 for actual data.

Double Parity (RAID 6)

Combines six or more drives in a way that protects data against loss of any two drives.

Striped (RAID 0)

Distributes data across several drives in a way that gives improved speed at any given instant.

None

Turns off data protection and leaves your data vulnerable to data loss.

4. Select a value for disk write caching.
5. Check **Enable periodic consistency check** to enable a monthly parity or mirror consistency check. The check helps to prevent a single drive failure from becoming a two-drive failure, resulting in data loss. The check runs for several hours and can affect performance of the px12-400r . If you do not want to run the check, uncheck this option.
6. Check **Use available drives as hot spares** to allow unused drives to become part of a RAID-protected storage pool. If a drive in a Storage Pool fails, all the data on that drive can be mirrored to the hot spare drive.
7. Click **Apply** to save your changes.

The Drive Management page displays a table that provides the following information about existing Storage Pools.

- **Name** — The name of the Storage Pool.
- **Protection** — The type of protection assigned to the Storage Pool.
- **Capacity** — The total amount of storage in the Storage Pool.
- **Used/Available** — Used is the space allocated to Shares. It is also space allocated to iSCSI drives. Available is the difference between capacity and used.

Drive status

An image on the Drive Management page provides information on the drive status of your px12-400r. The image displays the physical layout of drives and the drive slot numbers. If a drive has a circled letter, it is a member of a Storage Pool. If you hover your mouse over a drive in the image, the

ToolTip displays the drive model, size, and status, including if the drive is failing. If you hover your mouse on either a Storage Pool name in the table or on a drive in the Storage Pool image, all drives in the Storage Pool are highlighted.

How do I...

add Storage Pools
modify Storage Pools
delete Storage Pools
learn more about how content is stored

Backing up and Restoring Your Content

Backup and Restore Overview

Your Iomega StorCenter provides many ways to back up and restore content.

To back up content to and from your Iomega device, such as:

- Time Machine
- QuikProtect
- Copy Jobs

To back up and restore your Iomega device, there are:

- Copy Jobs
- Mozy Backup
- Avamar
- Amazon S3
- Iomega Personal Cloud features

Backup of Data through RAID Protection

The drives in your Iomega device are protected using a built-in, pre-configured technology that redundantly stores data across the drives. This technology, known as RAID (Redundant Array of Independent Disks), enables a series of drives to act together as a single storage system. For more information, refer to Understanding How Your Content Is Stored.

How do I ...

back up Macs with Time Machine
back up with Copy Jobs
back up with Mozy Backup
back up with Avamar
back up with Amazon S3
back up with Iomega Personal Cloud

Backing up to and Restoring from Your Device

Backing up Macs with Time Machine

You can back up your Iomega StorCenter px12-400r to Time Machine.

To set up Time Machine backups on an Iomega StorCenter px12-400r, run the Time Machine setup from the Mac you want to back up and follow these instructions:

1. Connect your Mac to your px12-400r using Apple File Protocol. You can do this using Iomega Storage Manager for Mac or Bonjour.
2. Mount the Backup Share from the Iomega network device.

   Note: If you want to create a new Share for Time Machine backups, you can do so using the Iomega StorCenter px12-400r Console.

3. Select System Preferences... from the Apple Menu.
4. Select Time Machine (listed under System).
5. Click ON to enable Time Machine.
6. From the list of available drives, choose the desired Share on your px12-400r, then click Use for Backup.

   Note: Time Machine uses a single destination drive for backups. If you have previously set up another drive for Time Machine backups and want to change to use the Iomega network device, click Select Disk, then choose the desired Share on your px12-400r.

   Note: Older Iomega Storage devices include a Time Machine feature. In more recent devices, the Time Machine feature is not included because it is no longer necessary to pre-configure a sparse bundle on the device. The sparsebundle image is created automatically when you complete Time Machine setup following the instructions above.

Copy Jobs Overview

You can back up content to and from your Iomega StorCenter using the Copy Jobs feature. Copy Jobs copies files from one storage device to another, either by a set schedule or immediately by the user. An example of a Copy Job scenario is if you keep pictures from your digital camera on a separate USB drive, but you also want to maintain a backup of these pictures on your Iomega device. Using Copy Jobs, you can create a task that copies your photos on the USB drive to a Share on your Iomega device, and you can set that task to a schedule so the images automatically copy at a specific time. This ensures that your photos are always safely backed up to your Iomega device in the event your USB device ever fails or is lost.

For more information, refer to Transferring Content to and from Your Iomega device.

How do I ...

add a Copy Job
manage a Copy Job
modify a Copy Job
delete a Copy Job
restore files with Copy Jobs

Backing up Your Device

Copy Jobs

Transferring Content to and from Your Iomega StorCenter px12-400r with Copy Jobs

You can transfer content to and from your px12-400r using the Copy Jobs feature. Copy Jobs copies files from one storage device to another, either by a set schedule or immediately by the user. An example of a Copy Job scenario is if you keep pictures from your digital camera on a separate USB drive, but you also want to maintain a backup of these pictures on your px12-400r. Using Copy Jobs, you can create a task that copies your photos on the USB drive to a Share on your px12-400r, and you can set that task to a schedule so the images automatically copy at a specific time. This ensures that your photos are always safely backed up to your px12-400r in the event your USB device ever fails or is lost.

Note: While a Copy Job copies all data from one NAS device to another, it does not copy permissions or access rights from one NAS device to another.

All saved Copy Jobs display on the Copy Jobs page. From there, you can manually start and stop a Copy Job, view Copy Job information, modify a Copy Job, check its last run status, and, if applicable, view when the Copy Job is next scheduled to run.

When defining a Copy Job, you can copy data from or to any of the following:

- Any NAS device automatically discovered on the same subnet as your px12-400r
- Any NAS device that you manually add to the subnet using the Iomega Storage Manager
- Any external storage device, such as a USB device, connected to your px12-400r
- A Windows computer that is automatically discovered on the same subnet as your px12-400r

When selecting what data to copy on the source storage device, you can choose a specific folder or all folders. You can also copy from a folder on an external storage device mounted to your px12-400r.

When selecting the destination device, you can copy files to the top-level folder on the destination device (the default option), or to an existing folder on this device, which adds the copied files into folders.

You can manually start or stop a Copy Job by clicking start or stop buttons on the Copy Jobs page. You can schedule a Copy Job to run automatically at a set day and time.

Copy Jobs Limitations

- Copy Jobs does not establish a continuous replication or mirroring relationship between the source and destination devices. You should not set up Copy Jobs for disaster recovery.
- Copy Jobs does not support transferring content from iSCSI drives.

Adding Copy Jobs

The page describes how to:

- Add Copy Jobs
- Set From Information
- Set To Information
- Set a Schedule

Adding Copy Jobs

1. On the Copy Jobs page, click . A Copy Job is added to the top of the list and the Information section displays.
2. Enter a name for the Copy Job.
3. The **Overwrite Setting** determines what happens to files in the destination location if they have the same name as those in the source location. Select one of the following values from the Overwrite Setting drop-down menu:
    - **Overwrite and don't delete** — Files in the destination location are overwritten with files from the source location. Any files in the destination location that are not in the source location are preserved.
    - **Overwrite and delete** — Files in the destination location are overwritten with files from the source location. Any files in the destination location that are not in the source location are deleted. The destination location becomes an exact copy of the source location.
    - **Don't overwrite** — Only files in the source location that are not in the destination location are copied. No files are overwritten in the destination location.

From: Settings

1. In the **From:** section, click to select a source location. This is the location of the files you want to copy. In the dialog, enter the Device Name or IP address in the text box, or select a device from the list. If a connected device is not listed, click the **Refresh** button.
2. Click **OK** to save your selection or click **Cancel**.
3. The **Protocol** drop-down menu displays if the source device is different from the device you are currently accessing; for example, it could be a separate NAS device on your network. From the **Protocol** drop-down menu, choose one of the following:
    - **Windows File Sharing** — The default value in the menu is Windows File Sharing and in most cases you should accept the default value. For more information, refer to Windows File Sharing.
    - **rsync** — The rsync protocol can provide faster copying, but may not be available on all devices. If you are able to select the rsync protocol, and you want the rsync Copy Job to be secure, select the **Use secure rsync (SSH)** option. Enter the rsync username and password for the rsync server to or from which you are copying. The rsync username and password is set up on a different device than the device on which you are creating the Copy Job. For more information on creating an rsync user, refer to rsync Server Settings.

4. Enter a valid username and password, if applicable, for the device to provide access to its folders.

5. To select a specific folder, click to select a source location for the **What to copy:** section. In the Copy dialog box, select all Shares or a folder, and select one of the following options for the Copy Job from the drop-down menu:

    - **The selected folder and its contents** — copies the selected folder and its contents. If the destination is a folder, a new folder will be created for each source folder. If the destination is Top Level, a new top-level folder is created on the destination device for each source folder.

    - **Only the contents of the selected folder** — copies the contents of the selected folder; not the folder itself. If the destination is a folder, the files and folders in the selected folder are copied directly to it (the source folder name is not copied). If the destination is Top Level, a new top-level folder is created on the destination device for each folder in the source folder.

6. By selecting Shares, you choose to copy All Shares, in which all files on the px12-400r are copied. Any files not contained in a folder are not copied. If the destination is a folder, a new folder will be created for each source folder. If the destination is Top Level, a new top-level folder is created on the destination device for each source folder.
7. Click **OK** to save your selection or click **Cancel**.
8. Click **Apply** to save your changes.

To: Settings

1. In the **To:** section, click to select a destination location. This is the location where you want your files copied. In the dialog, enter the Device Name or IP address in the text box. Or, from the drop-down menu, select a device in the list. If a connected device is not listed, click the **Refresh** button.
2. Click **OK** to save your selection or click **Cancel**.
3. The Protocol drop-down menu displays if the source device is different from the device you are currently accessing; for example, it could be a separate NAS device on your network. From the **Protocol** drop-down menu, choose one of the following:

    - **Windows File Sharing** — The default value in the menu is Windows File Sharing and in most cases you should accept the default value. For more information, refer to Windows File Sharing.

    - **rsync** — The rsync protocol can provide faster copying but, may not be available on all devices. If you are able to select the rsync protocol, and you want the rsync Copy Job to be secure, select the **Use secure rsync (SSH)** option. Enter the rsync username and password for the rsync server you are copying from or to. The rsync username and password is set up on a different device than the device on which you are creating the Copy Job. For more information on creating an rsync user, refer to rsync Server Settings.

4. Enter a valid username and password, if applicable, for the device to provide access to its folders.

5. To select a specific folder, click to select a destination location for the **Copy to here:** section. In the Copy to here dialog, select a Share or a folder from a Share to copy your files.
6. Click **OK** to save your selection or click **Cancel**.
7. Click **Apply** to save your changes.

Setting a Schedule

1. To set a schedule, expand the Schedule section.
2. In the Schedule section, select **Enable Schedule for Copy Job**.
3. Select the days you want the Copy Job to run, or select **All Days** to run the Copy Job every day.
4. Click to select a start time. Click **Done** to save your time selection.
5. Click **Apply** to save your changes. The new Copy Job displays on the Copy Jobs page.

How do I ...

manage a Copy Job
modify a Copy Job
delete a Copy Job
restore files with Copy Jobs

Managing Copy Jobs

From the Copy Jobs page, you can add, start, stop, delete, or monitor Copy Jobs.

After you have added Copy Jobs, the Copy Jobs page displays a list of Copy Jobs. The information section includes the name of each Copy Job, date and time it last ran, and its next scheduled time.

From the Copy Jobs list, you can perform the following actions:

1 Click to start a Copy Job.

2 Click to stop a Copy Job.

3 Click to delete a Copy Job.

4 Expand the **Copy Job Information** section to modify the Copy Job settings.

5 Click the **Schedule** section to view the Copy Jobs schedule.

How do I ...

add a Copy Job
modify a Copy Job
delete a Copy Job
restore files with Copy Jobs

Modifying Copy Jobs

1. In the list on the Copy Jobs page, find the Copy Job you want to modify, and click it to expand the **Information** section.
2. Refer to Adding a Copy Job for information about revising the Copy Job fields.

How do I ...

add a Copy Job
manage a Copy Job
delete a Copy Job
restore files with Copy Jobs

Deleting Copy Jobs

1. In the list on the Copy Jobs page, find the Copy Job you want to delete.
2. Click from the **Actions** column of the table to delete the Copy Job.

   The Delete Copy Job pop-up window opens.
3. If you are sure that you want to delete the Copy Job, click **Yes**.

   Note: If you do not wish to delete the Copy Job, click **Cancel** to return to the Copy Jobs page.

How do I ...

add a Copy Job
manage a Copy Job
modify a Copy Job
restore files with Copy Jobs

Restoring Files with Copy Jobs

To restore files with Copy Jobs, create a new Copy Job that reverses the back-up Copy Job. Modify the From and To settings to copy files from the backup location to the original source location, specify what to restore, set overwrite settings, and choose the protocol for the Copy Job.

Refer to Add A Copy Job for detailed information on Copy Job settings.

How do I ...

add a Copy Job
manage a Copy Job
modify a Copy Job
delete a Copy Job

Backing up with Mozy Backup

The Mozy online backup service allows you to create a Mozy account, connect your Iomega StorCenter px12-400r to the account, and back up Shares and folders to the Mozy cloud service.

Enabling Mozy Account Information

1. On the Mozy Backup page, click the switch on.

   Note: If you do not have a Mozy account, click the link to open an account.

2. Enter a valid email address, password, license key, and country for your Mozy account.
3. To upgrade your Mozy account, click the link.
4. Click **Apply** to save your changes.

Selecting Folders to Back Up

1. Expand the **Backup** section and select the Shares and folders to back up in the tree. The tree provides a way to select a Share and all its folders, or just some of the folders under a Share.
2. Click **Apply** to save your changes.
3. To create a scheduled backup, click **Backup schedule settings**.
4. In the Mozy Backup Settings dialog box, select one of the following:
   - **Automatic Backup** — to generate an automatic backup anytime you add a new file or change an existing file to your selected Shares or folders.
   - **Scheduled Backup** — to set up a scheduled backup.
5. If you are creating a scheduled backup, select the days you want the backup to run.
6. Enter the start or stop times for the backup, or click to select the times.
7. To prevent performance degradation on your px12-400r, select a speed limit for the backup.
8. To schedule the time that the backup will run at the selected speed, enter start and stop times.
9. Click **Apply** to save your changes.
10. Click **Apply** to save the selected Shares and folders to back up.

After a backup has completed, click **View log** to see which files have been successfully backed up by Mozy.

How do I ...

restore files with Mozy

Restoring Files with Mozy Backup

To restore folders and files with Mozy Backup:

1. Click the link to restore any files and folders you back up to your Mozy account.
2. Select the desired backup from the **Backup Date:** drop-down menu, either the latest backup or a previous one.

   The file browser provides a way to select a Share and all its folders, or just some of the folders under a Share.

3. Click **Apply** to save your changes.

   The Restore section displays a table with the status of a restore, either one in progress or one that has failed. To delete the restore task, click and confirm the deletion. When the restore finishes, the table status clears.

How do I ...

back up files with Mozy Backup

Registering with Avamar for Backup and Restore

Avamar is backup and recovery server software that uses deduplication to eliminate redundant copies of data, reducing the required storage space. For example, your Iomega StorCenter px12-400r might have 100 email messages with the same 1 MB attachment. If all those emails are backed up, that same attachment is backed up 100 times, requiring 100 MB of storage space. With Avamar and data deduplication, only one copy of the attachment is actually stored, so 100 MB of storage is effectively reduced to 1 MB.

Note: When you enable Avamar on your px12-400r, you are registering with an Avamar server. You cannot back up and restore from your px12-400r. Backup and restore operations are executed from the Avamar server.

Registering Your px12-400r with the Avamar Server

1. On the Avamar page, click the switch on.
   The Avamar Settings pop-up window opens.
2. In the Avamar Settings pop-up window, enter the following information and click **Apply** to save your settings:
   - **Server Address** — the Avamar server IP address or hostname.
   - **Client Domain** — the registered domain name from the Avamar server.

Backing up with Amazon S3

The Amazon S3 online storage service allows you to back up your Iomega StorCenter px12-400r to the cloud.

Enabling the Amazon S3 Feature

1. On the Amazon S3 page, click the switch on.

   Note: If you do not have an Amazon S3 account, click the link to create an account.

2. Enter a valid access key, secret key, and bucket name from your Amazon S3 account information.
   You can create a bucket at account setup, or you can enter a new bucket for your px12-400r. Your content lives in this bucket on your Amazon S3 account.
3. Select an existing Share on your px12-400r in which to copy files that are then backed up to Amazon S3.
4. Click **Apply** to save your changes.

Backing up Files to the Amazon S3 Cloud

After you copy files to the selected Share on your px12-400r, the files are automatically backed up to the Amazon S3 cloud service. File uploads are limited to 5 GB in size. If you delete files from the selected Share on your px12-400r, they are not automatically deleted from the cloud service. You can manually delete those files from the cloud service by clicking a command on the Amazon S3 page.

How do I ...

restore files with Amazon S3

Restoring Files with Amazon S3

When you want to restore files from the Amazon S3 cloud service to your Iomega StorCenter px12-400r, you can choose to restore all files or select individual files to restore.

How do I ...

back up files with Amazon S3

Backing up with Iomega Personal Cloud

You can back up content on your Iomega StorCenter by creating a Copy Job from the Iomega Personal Cloud on it to another Iomega device that is a member of the cloud.

Refer to Iomega Personal Cloud help for additional information.

How do I ...

create an Iomega Personal Cloud
create Copy Jobs with Iomega Personal Cloud

Restoring Files with Personal Cloud

You can restore content on your Iomega device by creating a Copy Job from the Iomega Personal Cloud on it to another Iomega device that is a member of the Personal Cloud.

Refer to Iomega Personal Cloud help for additional information.

How do I ...

create an Iomega Personal Cloud
create Copy Jobs with Iomega Personal Cloud

Securing Your Device and Contents

What Is Security and Do I Need It?

Security is an optional feature you can enable on your Iomega StorCenter px12-400r to secure Shares, create users, and allow some features to be enabled. When you create users, you limit access to your px12-400r to specific people, and when you secure Shares, you limit data access to specific users. Security adds an extra layer of protection to your px12-400r beyond whatever form of security you have on your local network. Without security, all data on your px12-400r can be accessed by anyone on your local network.

To secure your px12-400r:

- First enable security and create an administrator user.
- Create users. Create groups.
- Secure any existing or new Shares.
- Secure any existing or new iSCSI drives.

How do I...

enable security
add users
add groups
secure Shares

Enabling Security and Creating an Administrator User

With security turned on, only administrator users can view or change settings on the px12-400r, including creating or deleting users and Shares. When you create users, you limit access to your px12-400r to specific people, and when you secure Shares, you limit data access to specific users.

1. On the Security page, click the switch on.
2. When you turn security on, you will be asked to create an administrator user. Provide a username and password, and then confirm your password.
3. Encryption is always available when you access your px12-400r using https. By setting local encryption, you enforce encryption on your local network. By setting remote encryption, you enforce encryption outside your local network, such as through the internet. Choices for both encryption types are Not required, Passwords only (passwords are encrypted through https), and Always (encryption is always enforced). Always encrypting communication is safest, but can impact performance.

   Note: When security is turned on, browser communications with the px12-400r are encrypted. Therefore, each computer that attempts to access the px12-400r may encounter a security warning, which can be safely ignored. In addition, you may be asked to accept a signed certificate for the px12-400r, which you should accept. If you change the device name at a later date, these warnings may appear again.

   px12-400r administrators do not have access to all Shares by default. Access rights to Shares must be granted explicitly to administrators, as with other users.
4. If you have your own security certificate, you can load it by selecting **Use an imported certificate** and browsing to the certificate to load it.
5. Click **Apply** to save your changes.
6. Click here to learn how to create users.
7. Click here to learn how to secure any existing or new Shares.

Disabling Security

Disabling security will cause all defined users to be deleted.

Note: If you are using other features on your px12-400r that require security, you cannot disable security until those features are also disabled.

1. On the Security page, click the switch off.
2. Disabling security will cause all defined users and groups to be deleted. Check the box to disable security.
3. Click **Apply** to save your changes.

Security is disabled.

How do I...

create secured Shares
add users

Limiting Access to Your Content by Creating Users

When you create users, you are selecting the specific people that have access to your Iomega StorCenter. You can secure Shares and specify which users can read and write to the secured Shares. You can also create additional administrator users who can manage the Iomega device through the Iomega StorCenter Console. Administrator users can change various settings on the Iomega device, including adding and deleting Shares. If you create groups, you can also limit access to your Iomega device by group so you don't have to specify access for each individual user.

How do I ...

add users

add groups

Users

Users Overview

When security is enabled, the Users page displays all users on the Iomega StorCenter px12-400r and enables administrators to add and modify users.

Non-administrator users can be added to limit access to Share content. Additional administrator users can be added allow specific users to configure the px12-400r. The table displays the Usernames and Descriptive Name of each user. Click in a row of the table to view or modify details about a user.

How do I...

add users
manage users
delete users
create Shares for users

Adding Users

To add a user:

1. Navigate to the **Users** page.
2. Before you can create or modify users, you must have security enabled on your Iomega StorCenter Iomega device. If security is already enabled, you are ready to add users. If not, a pop-up window appears for enabling security and create an administrator user to manage your secured Iomega device.
3. To add a new user, click **Add a user**.
4. Enter the following information:
    - **Username** — enter the username of the user to be created. This is the username for logging into the Iomega device. There is a maximum of 32 characters, and spaces are not allowed. The following are not valid usernames: root, daemon, bin, sys, sync, mail, proxy, www-data, backup, operator, sshd, postfix, nobody, unuser, guest, and rsync.
    - **Descriptive Name** — add a descriptive name to identify the user. For example, if you created a user with a Username of jsmith, you may want to add the Descriptive Name Joe Smith.
    - **Password** — create a password for the user. The password should be between 8 and 12 characters, and spaces are not allowed.
    - **Confirm Password** — confirm the password. If the text in this field does not match the text in the Password field, an error will be returned.
    - **Quota Size** — set a quota size by entering a value in gigabytes. This limits the amount of storage space this user can have. To have no quota, leave this field blank.
    - **Administrator** — check this box to allow this user to manage the Iomega device.

      Note: An administrator does not have default access to all Shares. Access to Shares must be granted explicitly to all users, including administrators.

    - **Add a secured Share for this user** — check this box to create a secured Share for this user. This Share will have the new user's name, and allows access only to that user.
    - **Send a Personal Cloud invitation** — click this link to invite a user to join your Personal Cloud on the Iomega device. This opens the Send a Personal Cloud Invitation dialog box where you create an invitation by entering a user's email address along with any additional comments. A user then receives the invitation, which contains the Personal Cloud name and username and password. A user enters that information from Iomega Storage Manager. For more information on this, refer to the online help with Iomega Storage Manager. You see this option only if a Personal Cloud has been created on the Iomega device.
    - **Allow this user to add trusted devices to my Personal Cloud** — check this box to allow a user to join a trusted device to a Personal Cloud. A trusted device is a machine, either a computer or another Iomega device, that belongs to an added user. Only trusted devices that belong to users that have been added to the Iomega device can join the Iomega Personal Cloud. This option displays only if a Personal Cloud has been created on the Iomega device.
5. Click **Create**.

Managing Users

The page describes how to:

- Change User Information
- Change Access Permissions
- Set Quotas

Changing User Information

1. Modify the following information:
    - **Username** — enter the username of the user to be created. This will be the username provided when logging into the Iomega StorCenter px12-400r. There is a maximum of 32 characters, and spaces are not allowed. The following are not valid usernames: root, daemon, bin, sys, sync, mail, proxy, www-data, backup, operator, sshd, postfix, nobody, unuser, guest, and rsync.
    - **Descriptive Name** — add a descriptive name to identify the user. For example, if you created a user with a Username of jsmith, you may want to add the Descriptive Name Joe Smith.
    - **Password** — create a password for the user. The password should be between 8 and 12 characters, and spaces are not allowed.
    - **Confirm Password** — confirm the password. If the text in this field does not match the text in the Password field, an error will be returned.
    - **Send a Personal Cloud invitation** — click this link to invite a user to join your Personal Cloud on the px12-400r. This opens the Send a Personal Cloud Invitation dialog box where you create an invitation by entering a user's email address along with any additional comments. A user then receives the invitation, which contains the Personal Cloud name and username and password. A user enters that information from Iomega Storage Manager. For more information on this, refer to the online help with Iomega Storage Manager. You see this option only if a Personal Cloud has been created on the px12-400r.
    - **Allow this user to add trusted devices to my Personal Cloud —** check this box to allow a user to join a trusted device to a Personal Cloud. A trusted device is a machine, either a computer or another px12-400r, that belongs to an added user. Only trusted devices that belong to users that have been added to the px12-400r can join the Iomega Personal Cloud. You see this option only if a Personal Cloud has been created on the px12-400r.
    - **Quota Size** — set a quota size by entering a value in gigabytes. To have no quota, leave this field blank.
    - **Administrator** — check this box if you would like to allow this user to manage the px12-400r.

    - **Note**: An administrator does not inherently have access to all Shares. Access to Shares must be granted explicitly to administrators, as with other users.

    ---

2. Click **Apply**.

Changing Access Permissions

1. Expand **Access Permissions** to change Share access permissions for the selected user.
2. To give this user access to a specific set of Shares, click **Add access permissions**.
3. In the Add Access Permissions pop-up window, select which Shares this user can access, and click **Apply**.
4. Uncheck Read or both Read and Write to limit or deny access permission to each Share for this user.
5. Click **Apply** to save your changes. When both Read and Write are unchecked, the Share is removed from the list.

Setting Quotas

You can limit the amount of space allocated to one or more users by applying quotas.

Note: If your px12-400r has multiple Storage Pools and you define a quota for users, that quota is applied to all Storage Pools.

---

1. Click **Quota Settings** to enable quotas, and set a default quota for each user.
2. In the **Quota Settings** pop-up window, check **Enable quotas** to turn on quotas for each user.
3. If desired, enter a **Default Quota**. This quota applies to new users only.
4. Check **Set default quota for all users** to apply the default quota to all users.
5. Click **Apply** to save your changes.
6. To set individual user quotas, expand the **Information** section for a user and enter a value in **Quota size**. If you leave the box blank, there is no quota for that user.
7. Click **Apply** to save your changes.

Deleting Users

To delete a user:

1. From the Iomega StorCenter px12-400r Console, click **Users**.
2. To delete an existing user, click the username to expand the user.
3. In the User Information section, click **Delete**.
4. In the **Delete User** pop-up window, click **Yes**.
5. The user is removed from the user list.

Groups

Groups Overview

Groups consist of one or more users, and administrators can grant each group rights to Shares on the Iomega StorCenter px12-400r. Users can belong to more than one group. The Groups page enables administrators to create one or more groups, and grant each group rights to Shares on the px12-400r. Security must be enabled before you can create groups.

Note: Refer to the Security page to enable security permissions and create an administrator account, if you have not done so already.

By default, there are no groups defined. Once an administrator defines one or more groups, the Groups functionality is dynamically available when creating, modifying, and viewing users, Shares, and groups.

How Access Rights Are Granted Using Groups in Workgroup Mode

When groups are defined in Workgroup mode, a user's access rights are the most rights granted to the user and all groups to which the user belongs. For example, assume 3 Shares exist (SF1, SF2, and SF3), two users (UserA and UserB), and three groups (Group1, Group2, Group3). When created, UserA was not granted access rights to any Share, and UserB was granted Read rights to SF3. Group1 has Read/Write rights to SF1, Group2 has Read/Write rights to SF2, and Group3 has Read/Write rights to SF3. If UserA is added to Group1, UserB is added to Group2, and Group1 is added to Group3, the table below shows the resulting access rights for each user and group defined:

Name	Member of Group	Access Rights
UserA	Group1, Group3	SF1 - Read/Write SF3 - Read/Write
UserB	Group2	SF2 - Read/Write SF3 - Read
Group1	Group3	SF1 - Read/Write SF3 - Read/Write
Group2	none	SF2 - Read/Write
Group3	none	SF3 - Read/Write

How do I...

add new groups
add users
delete users

Adding Groups

1. On the Groups page, click **Add a group**. The Information section opens.
2. From the Information section, give the new group a name.
3. To add users to the group, click **Add users**. Select a user or users to include in the group. Select the checkbox in the title bar to add all listed users.
4. Click **Apply** to save your changes.

Managing Groups

The page describes how to:

- Remove a User from a Group
- Change Access Permissions

Removing a User from the Group

1. Open a group to display users belonging to it.
2. To remove a user from the group, click the next to that user. When the **Remove user** pop-up window appears, click **Yes** to remove the user.

Changing Access Permissions

1. To refresh the list of users, click above the table.
2. Expand **Access Permissions** to change group permissions to a secured Share. If iSCSI is enabled, you can also change group permissions to secured iSCSI drives.
3. To add permissions to a Share, click **Add access permissions**.
4. From the **Add Access Permissions** pop-up window, select a Share or Shares for the group to access. If iSCSI is enabled, select iSCSI drives for the group to access. Select the checkbox in the title bar to select all the Shares listed. If iSCSI is enabled, select the checkbox in the title bar to also select all the iSCSI drives listed.
5. Click **Apply** to save your changes.
6. In the table listing the Shares, check **Read** or **Write** for each Share. If iSCSI is enabled, check **Read** or **Write** for each iSCSI drive. The group can have full access by checking both **Read** and **Write**. To grant only read access, check only **Read**.

   Note: A group must have read access at a minimum. A group cannot have only write access.

7. Uncheck **Read** to remove all access to a Share and remove the Share from the table. If iSCSI is enabled, uncheck **Read** to remove all access to an iSCSI drive and remove the iSCSI drive from the table.
8. Click **Apply** to save your changes.
9. If NFS is enabled, the **GID** field is visible. The GID value must be the same on both the Linux client and the Iomega StorCenter px12-400r for the client to access files. To modify the GID, type a new GID value.

Deleting Groups

To delete a group:

1. From the Iomega StorCenter px12-400r Console, click **Groups**.
2. To delete an existing group, click to expand the group.
3. In the Information section, click **Delete** to delete the group.
4. In the **Delete Group** confirmation pop-up window, click **Yes**.
5. If you do not wish to delete the group, click **Cancel** to return to the Groups page.

Using Active Directory Domain to Manage Users and Groups

Active Directory Users and Groups Overview

On the Users and Groups page, administrator users can import users and groups from an Active Directory server and grant them access rights to Shares on the Iomega StorCenter px12-400r. The Users and Groups page is visible when you enable Active Directory on the px12-400r. For more information on enabling Active Directory on the px12-400r, refer to Configuring Your px12-400r to Use AD Domain. For information on creating an administrator user, refer to Enabling Security and Creating an Administrator User.

How do I...

enable security
change Active Directory settings
manage Active Directory users and groups
delete users and groups from Active Directory

Managing Users and Groups with Active Directory

The page describes how to:

- Import Users and Groups from Active Directory
- Synchronize with the Active Directory Controller
- Change Access Permissions
- Set Quotas

Importing Users and Groups from Active Directory

1. Click **Import Users and Groups from Active Directory**.
2. The pop-up window for **Import Users and Groups from Active Directory** is searchable, and you can sort by name, descriptive name, or type. You can filter the list of users and groups by selecting a specific user or group from the domain tree.
3. Select the checkbox next to a user or group to import that user or group to your Iomega StorCenter px12-400r from your Active Directory domain. Select the checkbox in the title bar to select all the users and groups in your Active Directory domain.
4. Click **Apply** to save your changes.

Synchronizing with the Active Directory Controller

You can poll the Active Directory controller at any time to check for new users and groups on the controller, so you can add them to your px12-400r. This keeps your px12-400r up to date with any group changes on the controller and indicates if any users on the controller were deleted or promoted.

Click **Synchronize with the Active Directory Controller**.

Changing Access Permissions

1. Expand **Access Permissions** to change user or group permissions to a secured Share. If iSCSI is enabled, you can also change user and group permissions to secured iSCSI drives.
2. To add permissions to a Share, click **Add access permissions**.
3. From the **Add Access Permissions** pop-up window, select a Share or Shares for the user or group to access. If iSCSI is enabled, select iSCSI drives for the user or group to access. Select the checkbox in the title bar to select all the Shares listed. If iSCSI is enabled, select the checkbox in the title bar to also select all the iSCSI drives listed.
4. Click **Apply** to save your changes.
5. In the table listing the Shares, check **Read** or **Write** for each Share. If iSCSI is enabled, check **Read** or **Write** for each iSCSI drive. A user or group can have full access by checking both **Read** and **Write**. To grant only read access, check only **Read**.

Note: A user or group must have read access at a minimum. A user or group cannot have only write access.

---

6. Uncheck **Read** to remove all access to a Share and remove the Share from the table. If iSCSI is enabled, uncheck **Read** to remove all access to an iSCSI drive and remove the iSCSI drive from the table.
7. Click **Apply** to save your changes.
8. If NFS is enabled, the GID field is visible. The GID value must be the same on both the Linux client and the px12-400r for the client to access files. To modify the GID, type a new GID value.

Setting Quotas

1. Click **Quota settings** to enable quotas and set a default quota. Quotas are only set for individual users, and not groups.
2. In the **Quota Settings** dialog, click **Enable quotas** to turn on quotas for each user. Quotas can be set for each user individually or set as a default value.
3. Enter a **Default Quota** in gigabytes. When you set a default quota, this becomes the quota size for all new users.
4. Check **Set default quota for all users** to globally set the same quota size to all users. You may overwrite this default value for individual users by setting their quota size separately in the user's Information section.
5. Click **Apply** to save your changes.

Deleting Active Directory Users and Groups

To delete a user or a group:

1. From the Iomega StorCenter px12-400r Console, click **Users and Groups**.
2. To delete an existing user or group, click to expand that user or group.
3. In the Information section, click **Delete**. Deleting a user or group does not delete any Shares to which the user or group has access. Click the checkbox if you want to **Delete all Shares that only this user can access**.
4. In the confirmation pop-up window, click **Yes**.
5. If you do not wish to delete a user or group, click **No** to return to the Groups page.

Personal Cloud: Accessing Your Device From Anywhere in the World

What Is an Iomega Personal Cloud ?

An Iomega Personal Cloud turns an Iomega StorCenter px12-400r into a hub for sharing files and backing up data among computers anywhere in the world. A Personal Cloud can exist on your Iomega StorCenter px12-400r, or on another Iomega network device. When you create a Personal Cloud, you gain access to your px12-400r from anywhere on the internet. You can also share with friends and family by inviting users to join your Personal Cloud. You manage Personal Cloud users the same way you manage other users on your px12-400r, so you control the storage and content they can access through the Personal Cloud. Trusted devices can be added to your Personal Cloud to connect them through the internet as if they are on a common home network with your px12-400r. People who join your Personal Cloud can access data, perform Copy Job operations, use your px12-400r as a QuikProtect remote target, stream media from your px12-400r over the internet, and use remote desktop to access computers on the local network for your px12-400r. If you allow a user to join their trusted devices to the Cloud, those devices become part of the Cloud and can be accessed by other users on the Cloud.

Iomega Personal Cloud Key Terms

The following are a few key terms to help get you started with a Personal Cloud:

- **Iomega Personal Cloud** — This is a setting configured on your Iomega StorCenter px12-400r Console that allows you to securely share storage and media capabilities with computers around the world.
- **Web Access** — You can use Personal Cloud information to access your px12-400r from the web. Enter myCloudName.Myiomegacloud.com in a web browser, and when prompted, enter a valid username and password for your px12-400r. You can also use the Iomega Link, which is an application that runs on mobile devices, by entering the Personal Cloud name and then a valid username and password. For more information on the Iomega Link, refer to its documentation.
- **My Personal Cloud** — When you are the administrator of an px12-400r, you can create a Personal Cloud through the Iomega StorCenter px12-400r Console and then invite people to join it. You create and manage the Personal Cloud on your Iomega StorCenter px12-400r Console through the **My Personal Cloud** configuration option. The Personal Cloud that you administer is called My Personal Cloud.
- **Other Personal Cloud** — If you want to have your px12-400r join that Personal Cloud instead of administering your own, select the option for **Other Personal Cloud**. Enter the Personal Cloud name, username and password you received when you were invited to join your px12-400r as a Trusted Device on the other Personal Cloud.
- **Joining an Iomega Personal Cloud as a Trusted Device** — To connect your computer or your px12-400r as a trusted device to a Personal Cloud, you use the username and password given to you for that Personal Cloud. The person managing the Personal Cloud has to create you as a user on the device hosting the Personal Cloud and give you permission to add trusted devices. You can connect your px12-400r to only one Personal Cloud at any given time, so you must select between either My Personal Cloud or Other Personal Cloud.

An administrator should complete the following tasks to set up or join a Personal Cloud:

- create a Personal Cloud
- invite people to a Personal Cloud
- join a trusted device to a Personal Cloud

Is My Content Secure?

Your content is always secure using an Iomega Personal Cloud. If you create a Personal Cloud with security disabled, you are required to enter a password when accessing your Iomega device remotely. Enabling security allows you to share your Iomega device with the people you choose. For example, you have photos of your new baby you want to share with your sister, your brother, and your sister-in-law. To share your baby photos with these family members, create a Personal Cloud, and then invite your sister, your brother, and your sister-in-law to join your Personal Cloud. Your Iomega StorCenter provides an easy way to send email invitations and instructions to the people you select as Personal Cloud users. In this way, your content is never exposed to the public, and remains private. It is visible only to the individuals you invite to be Personal Cloud users. Content of the Personal Cloud is determined by you as the Personal Cloud owner. Refer to the help topic links below for more information on Personal Cloud.

Note that people added to your Personal Cloud as users are not required to own or have access to an Iomega device. The process of adding someone as a Personal Cloud user grants them access to your Personal Cloud from any computer.

How do I ...

create an Iomega Personal Cloud
configure a router for port forwarding
create a Personal Cloud
invite people to a Personal Cloud
join a trusted device to a Personal Cloud
enable security on Iomega device

Iomega Personal Cloud Setup Overview

You can create an Iomega Personal Cloud in one of two ways:

- Follow the Iomega Personal Cloud setup through Iomega Setup
- Create the Iomega Personal Cloud through the Iomega StorCenter Console

Creating an Iomega Personal Cloud starts with providing a name for your Personal Cloud and an email address associated with it. After creating the Personal Cloud, you can use the Personal Cloud Quick Setup wizard to perform common tasks associated with the Iomega Personal Cloud: adding Shares, inviting people to join the Personal Cloud, and setting up Copy Jobs through the Personal Cloud.

How do I ...

enable security on my Iomega device
create an Iomega Personal Cloud
configure a Personal Cloud
invite people onto your Personal Cloud
join a trusted device to a Personal Cloud
use Copy Jobs with a Personal Cloud

Creating an Iomega Personal Cloud

Before you can work with your Iomega Personal Cloud, you first create a Personal Cloud and configure the settings.

After your Personal Cloud is ready and connected to the internet as indicated by the status images, you can invite people to join your Personal Cloud. When you invite people to join your Personal Cloud, you add them as users on your Iomega StorCenter. The invited users receive an email invitation that includes the username and password they must provide when connecting to the Personal Cloud from the Iomega Storage Manager on their computer.

If you have content on your Iomega device that you do not want to share with members of your Personal Cloud, you should put that content in secured Shares that are not accessible to anyone invited to your Personal Cloud.

Note: This procedure assumes you did not create a Personal Cloud using the initial Iomega Setup portal. If you have already created a Personal Cloud, you do not have to follow this procedure.

---

1. On the Iomega Personal Cloud page, expand the **Configure** section.
2. Click the **My Personal Cloud** button to open the portal that lets you create your Personal Cloud.

   After you click the My Personal Cloud button, a new website containing the portal opens. You create a Personal Cloud on this website. After you create the Personal Cloud, you return to the Iomega StorCenter Console.

3. If your Iomega device is not secured, you are prompted to create a remote access password. This is a password that anyone not on your local network must enter to access your device.

   After completing these steps, the Personal Cloud Quick Setup Wizard opens, so you can create Shares, invite users, or configure Copy Jobs. You can use the Quick Setup Wizard or close it and begin using your Personal Cloud.

How do I...

invite people to a Personal Cloud
join a trusted device to a Personal Cloud
enable security on Iomega device

Configuring Router Port Forwarding for Personal Cloud

In most cases, your Iomega StorCenter attempts to automatically configure your router. However, if it cannot, a message displays that your router is not configured for port forwarding, and you must manually configure your router to forward a specific port to your Iomega device. Most routers refer to this as port forwarding, application access, or virtual server. It is recommended that you refer to your router's documentation for setting these values. When you set up port forwarding, you are allowing data to travel through your Personal Cloud between your Iomega device and trusted devices.

When you have selected a port value to forward for Personal Cloud, click **Settings** on the Personal Cloud page, and enter your selected port number in the Personal Cloud settings dialog box. If you have more than one Personal Cloud, you can enter a range of port values for your Personal Clouds. The range of port values is 50500-50599. You must also port forward port 443 to enable https access to your Iomega device.

Router Port Forwarding

Some routers have a UPnP option. If you have a UPnP router, enabling this option allows the Iomega device software to automatically configure the correct forwarding ports. Otherwise, you must perform additional steps by manually enabling port forwarding on your home network router. Port forwarding allows invited users to connect remote computers or other Iomega device devices outside of your local area network (LAN) as trusted devices to the Personal Cloud on your network.

Note: Port forwarding must be configured for both the network router on which the Personal Cloud is configured, and any remote network from which trusted devices are accessing the Personal Cloud.

The following steps are generic router settings. If you have never logged into your router before, you must consult the manufacturer’s documentation to find specific details such as default IP address, default administrator account, and password.

1. Log in to your router by entering its IP address in the browser’s URL field from your computer. If prompted, enter administrator account name and password.
2. Navigate to the Port Forwarding configuration page. This is often related to Port Mapping, Application, Virtual Server, or Gaming configuration options.
3. Type in the desired application or service name. This is typically a blank or drop-down field where you can type or choose a user-specified application or service name for the port you are forwarding. Create a new entry with a value like “Iomega Personal Cloud ” in this field.
4. Enter a port number for the Personal Cloud service in the range 50500-50599 in both the port start and port end fields. Port number 50500 is the default. It should not be necessary to change this value, but if you do, choose the next available port; for example, 50501. If you decide to choose a port in the higher range, note that the Media Server uses the same range of ports, numbering backwards from 50599.
5. Repeat the previous step, using port 443 to enable https communication with your Iomega device.
6. Enter the IP address of your Iomega device which contains the Personal Cloud. The IP address displays on the System Status page when you log into the device's web interface.
7. Save the changed settings.
8. Reboot the router if required.

How do I ...

create an Iomega Personal Cloud

Configuring Your Iomega Personal Cloud

As an Iomega Personal Cloud administrator, you can manage various settings on your Personal Cloud to ensure that it functions as efficiently as possible. Settings include specifying an email address when sending invitations. When data is traveling through the Personal Cloud, you can control the security of that information by specifying a Secure Communication level. Note that data stored on your px12-400r through the Personal Cloud is not encrypted, and using encryption can slow down communications.

Enabling Internet Access to the px12-400r

You can grant internet users, including Iomega Link users, secure access to the web interface and unrestricted access to media content on your px12-400r. Iomega Link is an application that runs on mobile devices, and allows access to content on your px12-400r. Before enabling secure access, you must first enable security on your px12-400r and create users. After enabling secure access, any internet users can access your px12-400r, and view any public content. Secure content is restricted to internet users who have valid usernames and passwords for the px12-400r. When you enable unrestricted media content access, your media files become available to all internet users.

Changing Personal Cloud Settings

1. In the Configure section of the Personal Cloud page, click **Settings**.
2. In the Personal Cloud Settings dialog box, configure the following:
    - **Administration Email Address** — This is the sender email address used on the email invitations.
    - **Port Number** — Your router forwards this specific port for your Personal Cloud. This value is automatically filled in, and you do not have to change it, unless you have more than one Personal Cloud on your network. Refer to Configuring Router Port Forwarding for Personal Cloud for more information.
    - **Secure Communication** — This setting controls the security of information traveling through the Personal Cloud.

      Note: You can also specify a Secure Communication level setting with Iomega Storage Manager. The Secure Communication setting for the Iomega StorCenter px12-400r Console sets the minimum value. You cannot specify a setting lower than this value using Iomega Storage Manager. For information on using Iomega Storage Manager, refer to its online help.

    - **Enable unrestricted access to media content** — This setting makes all media files in media-enabled Shares available to anyone on the internet accessing your px12-400r, even if those media files are in secured Shares. For mor information on making a Share media-enabled, refer to changing Share information.
3. Click **Apply** to save your changes.

How do I...

create a Personal Cloud
configure a router for port forwarding
invite people onto your Personal Cloud
join a trusted device to a Personal Cloud
manage trusted devices on a Personal Cloud

disable or delete my Personal Cloud
enable security on px12-400r
enable the Home Page

Inviting People onto Your Iomega Personal Cloud

When you invite people to join your Iomega Personal Cloud, you are actually selecting from existing users on your Iomega device, or adding people as users on your Iomega device. In addition, you are optionally allowing them to add their computers or Iomega storage devices as trusted devices on your Personal Cloud. Computers are added as trusted devices through Iomega Storage Manager. Refer to its online help for more information.

1. From either the Personal Cloud Quick Setup dialog box or the Iomega Personal Cloud page, click **Invite Users**.

   Note: You can also send an invitation to join a Personal Cloud when you are adding users. Refer to Adding Users for more information.

2. In the Invite Users dialog box, select the name of an existing user or click **Create New User** to add a new user. If security has not been enabled, you are prompted to enable security and create an administrator user.
3. If the email address field is not already completed, enter an email address for the user.
4. Click **Apply** to send the invitation.

How do I ...

create an Iomega Personal Cloud
add users to my Iomega device

Joining a Trusted Device to an Iomega Personal Cloud

You can join your Iomega StorCenter px12-400r to the Personal Cloud as a trusted device if you have been given permission by the person administering the Personal Cloud.

Note: You cannot join your trusted device to a Personal Cloud if you have not been added as a user on the Personal Cloud.

1. On the Personal Cloud page, select the **Other Personal Cloud** command to join another Iomega Personal Cloud.
2. In the Add Trusted Device to Personal Cloud dialog box, enter the Personal Cloud name, username, and password you received in the email invitation.
3. Enter a descriptive name for your trusted device in the Description field.
4. Click **Apply**.

After applying this information, you are automatically connected to the Personal Cloud.

How do I ...

enable security on my px12-400r
create an Iomega Personal Cloud
configure a Personal Cloud
invite people onto your Personal Cloud
use Copy Jobs with a Personal Cloud
delete a trusted device

Managing Trusted Devices on a Personal Cloud

As an Iomega Personal Cloud administrator, you can manage trusted devices on your Personal Cloud. Trusted devices can be disconnected, or you can completely delete a trusted device from the Personal Cloud.

Disconnecting Trusted Devices

Click **My Personal Cloud**, and expand the trusted device section of the page.

To disconnect a trusted device from the Personal Cloud, disable the trusted device by clicking the switch to Disabled, and click **Yes** in the confirmation pop-up window. The trusted device is not deleted and can be reenabled at a later time.

Deleting Trusted Devices

To delete a trusted device from the Personal Cloud, click next to the device's name. The trusted device is deleted and can only be added again by a user with trusted device privileges.

1. On the Personal Cloud page, expand the Trusted Devices section.
2. Click next to the trusted device you want to remove from the Personal Cloud.
3. Confirm the deletion.

How do I ...

join a trusted device
enable security on my px12-400r
create an Iomega Personal Cloud
configure a Personal Cloud
invite people onto your Personal Cloud
use Copy Jobs with a Personal Cloud

Using Copy Jobs with an Iomega Personal Cloud

You can create Copy Jobs that can transfer data from one trusted device to another through the Personal Cloud. When you add a trusted device to your Personal Cloud, a Copy Jobs icon displays next to that device in the trusted device table. Clicking the Copy Jobs button opens the Copy Jobs page to help you configure a Copy Job between the Iomega StorCenter px12-400r that is hosting the Personal Cloud and a trusted device. For more information on setting up Copy Jobs, refer to Adding Copy Jobs.

How do I...

create a Personal Cloud
join a trusted device to a Personal Cloud
add a Copy Job
enable security on px12-400r

Disabling or Deleting Your Iomega Personal Cloud

When you disable your Personal Cloud, you are eliminating access to your Personal Cloud without deleting the account information you created when you set up the Personal Cloud. Later, if you want to reenable your Personal Cloud, you can without reentering all the account information. To completely stop the Personal Cloud and eliminate any account information with it, delete it. If you delete your Personal Cloud and later decide you want to recreate it, you must start the creation process again and re-invite all users. When you delete a Personal Cloud, you lose your ownership of its name.

To disable a Personal Cloud, click **Disable**.

To delete a Personal Cloud, click **Settings** and then click **Delete** in the Personal Cloud Settings dialog box.

How do I...

create a Personal Cloud
invite people onto your Personal Cloud
join a trusted device to a Personal Cloud
configure my Personal Cloud
enable security on px12-400r

Accessing Content Using Your Iomega Personal Cloud

You can share content by inviting users to your Personal Cloud. The data in Shares can be made accessible to all users of the Cloud, or access can be restricted to a specific set of users by setting access permissions to Shares. Access permissions control whether users are only allowed to read files in Shares, or if they can also write (upload) files to Shares.

How do I ...

create an Iomega Personal Cloud
add users
create Shares
set access permission for Shares

Informing Users What to Do with Iomega Personal Cloud

Personal Cloud enables users to access your Iomega device from the web. They can enter myCloudName.Myiomegacloud.com in a web browser, and when prompted, enter a valid username and password for your Iomega device. After they access your Iomega StorCenter, they can view Shares, upload and download content, and stream content. Optionally, they can install Iomega Storage Manager on their computers, and then join their computers as trusted devices to the Personal Cloud. When users join their computer as a trusted device to the Personal Cloud, they are making their machine and its files available to other users of the Personal Cloud. A large virtual network is created.

How do I ...

create an Iomega Personal Cloud
add users
invite people to a Personal Cloud
join a trusted device to a Personal Cloud
enable security on Iomega device

Sharing Content Using Social Media

Sharing Content Using Social Media: Overview

If you have an account with social media services such as Facebook, Flickr, or YouTube, you can share content on your Iomega StorCenter px12-400r with your friends and family using one or more of these social media sites. To share your content using social media sites, create Shares called Active Folders, and connect each Active Folder with a social media account. Refer to the help topic links below for more information on these procedures. When you add photos and movies to an Active Folder, those files are automatically uploaded to the social media site associated with that Active Folder. If you have photos or movies you want to share with others, this is a great way to make your content available to people who may not have access to your px12-400r.

If you have configured a Personal Cloud on your px12-400r, you can grant Personal Cloud users access to Shares and Active Folders. This is useful if you want to allow users to add files to your social media sites. For example, if your px12-400r has a Flickr Active Folder, you can grant Personal Cloud users access to that Active Folder. In this manner, when photos are added to the Flickr Active Folder, either by you or by Personal Cloud users, those photos are uploaded automatically to your Flickr account.

Note that an Active Folder can only be associated with one social media account. For example, if you want Active Folders for your Facebook and YouTube accounts, create two Active Folders, and assign one Active Folder to Facebook, and one to YouTube. Using this example, any photos you add to your Facebook Active Folder are automatically uploaded to your Facebook page, and any movies you add to your YouTube Active Folder are automatically uploaded to your YouTube page. Not only is this a fast and easy way to share content, but uploading content to your social media sites provides an additional backup of your content, as the content is stored both on your px12-400r and at your social media accounts.

How do I...

make a Share an Active Folder
upload to Facebook
upload to Flickr
upload to YouTube

Facebook

Facebook is a social network to connect with friends and family. You can configure a Share as a Facebook Active Folder so that photos and movies added to that Share are automatically uploaded to your Facebook account.

Refer to Managing Shares for more information on managing Shares and Active Folders.

Note: If you do not have a Facebook account, go to the Facebook website to open an account.

Configuring a Facebook Active Folder

1. From the Iomega StorCenter px12-400r Console, click **Shares**.
2. Select a Share to use as a Facebook Active Folder, and click to expand the Active Folder section.
3. Check **Enable**.
4. Select **Facebook** from the drop-down menu.
5. Click **Configure Facebook account access** to configure your Facebook account. You will be taken to a Facebook page to configure your account. Follow the instructions provided by Facebook.
6. Check **Delete files after upload** to delete images or movies from the Share once they are transferred to your Facebook account.
7. Images can also be resized prior to upload. Check 800x600, 1024x768, or enter a custom resolution for resizing images.
8. Click **Apply** to save your changes.

   Once configured, all your images in this Active Folder will upload to your Facebook account.
9. Click **View Transfer History** to see the transfer activity from this Share to your account.

How do I...

add a Share
make a Share an Active Folder

Flickr

Flickr is a photo sharing network for sharing photos with friends and family. You can configure a Share as a Flickr Active Folder so that images and albums added to that Share are automatically uploaded to your Flickr account.

Refer to Managing Shares for more information on managing Shares and Active Folders.

Note: If you do not have a Flickr account, go to the Flickr website to open an account.

Configuring a Flickr Active Folder

1. From the Iomega StorCenter px12-400r Console, click **Shares**.
2. Select a Share to use as a Flickr Active Folder, and click to expand the Active Folder section.
3. Check **Enable**.
4. Select **Flickr** from the drop-down menu.
5. Click **Configure Flickr account access** to configure your Flickr account. You are taken to a Flickr page to configure your account. Follow the instructions provided by Flickr.
6. Check **Delete files after upload** to delete images from the Share once they are transferred to your Flickr account.
7. Click **Apply** to save your changes.
8. Once configured, all images added to this Active Folder are uploaded to your Flickr account. Click **View Transfer History** to see the transfer activity from this Share to your account.

How do I...

add a Share
make a Share an Active Folder

YouTube

YouTube is a social media site to share video content. You can configure a Share as a YouTube Active Folder so that videos added to that Share are automatically uploaded to your YouTube account.

Refer to Managing Shares for more information on managing Shares and Active Folders.

Note: If you do not have a YouTube account, go to the YouTube website to open an account.

Configuring a YouTube Active Folder

1. From the Iomega StorCenter px12-400r Console, click **Shares**.
2. Select a Share to use as a YouTube Active Folder, and click to expand the Active Folder section.
3. Check **Enable**.
4. Select **YouTube** from the drop-down menu.
5. Check **Delete files after upload** to delete videos from the Share once they are transferred to your YouTube account.
6. Click **Apply** to save your changes.

   Once configured, all videos added to this Active Folder automatically upload to your YouTube account.

7. Click **View Transfer History** to see the transfer activity from this Share to your account.

How do I...

add a Share
make a Share an Active Folder

Share Content through Iomega Personal Cloud

You can share your multimedia content with friends and family through an Iomega Personal Cloud. Refer to the Iomega Personal Cloud section for more information.

How do I ...

create an Iomega Personal Cloud
know my Personal Cloud content is secure

Media Management

Media Management Overview

The px12-400r has a built-in media server that, when turned on, scans for media content in specific Shares that have media sharing enabled. Any media content contained in these specific Shares are accessible to any user on your network with a media player, even if the Share is secured. For information on enabling a folder as a media folder, refer to Managing Shares.

Scanning for media content

The Media Server automatically scans for media content on a regular basis. However, you can click **Scan now** at any time to force the media server to perform an immediate scan for media content. This is especially useful after you have created new folders with media sharing enabled and copied a large amount of media content to them.

How do I...

share media content over the internet
enable media aggregation
stream music, movies, and pictures
share media through social media

Media Services Capabilities and Limitations

One important consideration when using the media server is that it can share media content on your px12-400r with anyone on the internet. When media sharing is enabled, internet users, including those users on mobile devices running the Iomega Link, can access media content on your px12-400r.

Note: When you enable internet access to your media content, all media content is available to any user on the internet, regardless of any security you may have applied to a media file. All your pictures, movies, and music are available to anyone accessing your px12-400r. You should be sure you want to make all your media content this accessible.

Sharing Media Content over the Internet

There are two methods for sharing media content on your Iomega device with anyone on the internet. You can enable internet access on the Media Server page. Alternatively, you can enable internet access by configuring your Iomega Personal Cloud.

Enabling Internet Access from the Media Server Page

Note: You can only enable internet access from the Media Server page if you have already created and configured a Personal Cloud. If a Personal Cloud is not set up, you do not see the Enable internet access option.

1. On the Media Server page, click **Settings**.
2. In the dialog box, check **Enable internet access**.
3. Click **Apply** to save your changes.
4. In the confirmation dialog box, check **Check this box to continue**.
5. Click **OK** to save your selection or click **Cancel**.

To access media content, internet users enter a non-secure IP address in their browser along with the port number 9000 used to access the media server, for example, http://72.xx.xxx.104:9000, where "x" is the IP value for your network. When a user enters this IP address, the Twonky Server page on the Iomega device displays. Refer to the Support section of the Twonky Server page for information on using the server. Iomega Link users can access media content directly from the Iomega device. Refer to your Iomega Link documentation for details.

For additional information on enabling internet access, refer to Media Services Capabilities and Limitations.

How do I...

scan for media content
enable media aggregation
stream music, movies, and pictures

Media Aggregation

If you have multiple Digital Living Network Alliance (DLNA) servers in your network that have media content, you can combine all media content into one view by enabling aggregation on your Iomega device. When you enable aggregation, all media content on DLNA servers is available for playback using a DLNA player, such as Playstation®3, Windows Media Player®, or Xbox 360®. In addition, you can optionally copy all media content from your network servers to your Iomega device.

Enabling Media Aggregation

1. On the Media Server page, click **Settings**.
2. Check **Enable media aggregation**.

   This enables aggregation for media servers already discovered in your network.

3. Choose the default aggregation setting.

   The default aggregation setting sets the default value for media servers as they are added to your network.

The default aggregation settings are as follows:

- **None** — Media aggregation is off.
- **Show Common View** — This enables media aggregation and allows all media content from computers on the network to be played back by a DLNA player. All your movies, music, and pictures are linked from various computers and can be played back from one view. All aggregated media files remain on their original device, and can only be played while that device is powered on and connected to the network.
- **Copy Files** — This enables media aggregation and automatically copies all media content from computers, both networked and local, to your Iomega device. All your movies, music, and pictures from various computers can be played back from one view, and they are copied into Shares on your Iomega device. Because all media files are copied to the Iomega device, they can be played even if the original device they were on is powered off or not connected to the network.
- **Copy on Request** — This enables media aggregation but does not automatically copy all media content from computers, both networked and local, to your Iomega device. Computers on the network will have to enable media aggregation individually and then media files are copied to the Iomega device. If a computer is running the Iomega Storage Manager, media aggregation is automatically enabled.

Note: When you enable media aggregation, the media server restarts, and any media you are currently streaming stops playing. You can begin streaming your media after the media server has restarted.

Social Media Sharing

You can share media content, such as movies and pictures, using social media sites like Facebook, Flickr, or YouTube. Refer to the Sharing Content Using Social Media section for more information.

How do I ...

share content through Facebook
share content through Flickr
share content through YouTube

Streaming Music, Movies, and Pictures

The Media Server supports playback of videos, music and pictures from any UPnP AV (Universal Plug and Play Audio Visual) network media players, such as Playstation3, Windows Media Player, or Xbox 360.

You can play back all your media files from your individual home computers by enabling media aggregation on your Iomega device. You can also connect USB mass storage devices (such as your iPod, mp3 player, or USB drive) to your Iomega device and directly stream files through the device, or access media files through a networked media player. Below are two examples of how to set up the following media players:

- iTunes
- Xbox 360

Note: The procedures shown below are intended as examples. Your media player or version may operate differently. It is recommended that you refer to your media player documentation for instructions on how to add a network device.

Example: Setting up iTunes

1. Locate the source directory of your iTunes media content.
2. Drag, or copy, your existing media content to a Share that has media sharing enabled.
3. When you open the iTunes Library, iTunes will display all of the media content from the Iomega device.

Example: Setting up Xbox 360

1. Connect your Xbox 360 to your TV and to the same local network as your Iomega device.
2. Navigate to the **Media** Tab in Xbox 360 and select a media-enabled Share.
3. Select **Computer** from the options menu.
4. Click **Yes, Continue** when asked if you have downloaded and installed media sharing software on your computer, since the Iomega device device comes preconfigured with this software.
5. Select Iomega device from the list of names. You should now see all the public media content on your device.

How do I ...

enable media aggregation
learn more about social media sharing

Photos

Photos Overview

Your Iomega device has multiple ways to manage your pictures.

Your Iomega device can:

- Stream pictures that are in Shares with media sharing enabled
- Display pictures on the Home Page in a slideshow
- Automatically resize pictures
- Transfer pictures from your digital camera
- Upload pictures to social media sites like Flickr or Facebook

---

How do I ...

stream pictures
display pictures in a slideshow
automatically resize pictures
transfer pictures from a digital camera
upload pictures to Facebook
upload pictures to Flickr

Streaming Pictures

The Iomega StorCenter has a built-in media server that, when turned on, can scan for pictures in specific folders that have media sharing enabled. Any pictures contained in these specific folders will then be accessible to any user on your network with a media player. For information on enabling a folder as a media folder, refer to Managing Shares.

Scanning for Pictures

The Media Server automatically scans for media content on a regular basis. However, you can click **Scan now** at any time to force the media server to perform an immediate scan for pictures. This is especially useful after you have created new folders with media sharing enabled and copied a large amount of media content to them.

How do I ...

display pictures in a slideshow
automatically resize pictures
transfer pictures from a digital camera

Creating a Slideshow on the Device Home Page

Your px12-400r can display a slideshow on its home page.

On the Home Page Settings feature page, check **Display slideshows** to display picture slideshows from folders on the px12-400r. Click **Manage slideshows** to configure any slideshows you want to display. The slideshow location can be any folder attached to the px12-400r, including a USB drive or DFS location.

Automatically Resizing Your Photos

A Photo Resize Active Folder automatically changes the size of photos in that Share to a set size. You can choose to keep the original photos added to this Share, while a resized copy is created. The resized photos are saved to a folder on the Share named by the photo size you choose, such as 800x600. To configure a Share as a Photo Resize Active Folder, access Shares from the Iomega StorCenter px12-400r Console, select a Share, and expand the Active Folders section to enable and configure it.

Refer to Managing Shares for more information on managing Shares and Active Folders.

Configuring a Photo Resize Active Folder

1. From the Iomega StorCenter px12-400r Console, click **Shares**.
2. Select a Share to use as a Photo Resize Active Folder, and click to expand the Active Folder section.
3. Check **Enable**.
4. Select **Photo Resize** from the drop-down menu.
5. You can set a size for your pictures. Select 640x480, 800x600, 1024x768, or enter a Custom Resolution for resizing images. The resized photos are saved to a folder on the Share named by the photo size you choose, such as 800x600.
6. You can keep a copy of the original by selecting **Keep the original files after resizing**.
7. To add a watermark to your photo, select **Add a watermark to the photos**. Click the Watermark file icon to apply a watermark image to your file.
8. Click **Apply** to save your changes.
9. Once configured, all photos added to this Active Folder are resized to your settings. Click **View Content** to see the files in this Share.

How do I...

manage a Share

Getting Pictures from Your Camera

The Picture Transfer Protocol (PTP) allows pictures to be automatically copied from a USB camera connected directly to the px12-400r. When Picture Transfer is turned on, and your camera is connected to your px12-400r, the pictures are copied to the configured destination folder.

1. Open the Picture Transfer page, click the switch on.
2. Optionally, if you want to automatically delete the pictures from your camera once they have been safely copied to your Iomega StorCenter, check **Remove Copied Pictures From Camera** to automatically delete the pictures from your camera once they have been safely copied to your px12-400r.
3. Click to open the Select Folder pop-up window, and select a Share as the destination for your pictures.

Music

Music Overview

If you have music files in media-sharing enabled folders on your Iomega device, those music files can be streamed by a DLNA player running on a computer on the network.

How do I ...

stream music

Streaming Music

The Iomega StorCenter has a built-in media server that, when turned on, scans for music in specific folders that have media sharing enabled. Any music contained in these specific folders is then accessible to any user on your network with a media player. For information on enabling a folder as a media folder, refer to Managing Shares.

Scanning for Music

The Media Server automatically scans for media content on a regular basis. However, you can click **Scan now** at any time to force the media server to perform an immediate scan for media content. This is especially useful after you have created new folders with media sharing enabled and copied a large amount of media content to them.

Torrents

Torrent Overview

Torrent downloads allow you to share files using a peer-to-peer file sharing protocol. With torrent download enabled, you can download files using the torrent protocol to your Iomega StorCenter and then those files can be uploaded by other torrent users.

After you have added torrent jobs to your torrent share, the torrent download page displays a table of torrent jobs, showing both downloads and files available for upload. Multiple torrent files can download simultaneously. The table information includes the name of the file, its size, download or upload status, and amount of time remaining for the torrent job to complete.

How do I ...

enable torrent downloads
configure a router for torrent downloads
delete torrent jobs
share torrent downloads with other peers
add torrent files to your Iomega StorCenter

Enabling Torrent Downloads

1. On the Torrent Download page, click the switch on.
2. Click **Settings** to modify the torrent download and upload settings.
3. In the Torrent Download Settings dialog box, enter a value for **Maximum Download Speed**. This sets the rate at which files are downloaded to your device. The maximum download speed you can enter is 2 MB/s.
4. Enter a value for **Maximum Upload Speed**.
   This sets the speed at which other users can upload a file unprompted from your device. The upload speed can affect device performance, so it is recommended that you choose a value that does not strain the performance of your device and impact other work on it. The maximum upload speed you can enter is 1GB/s.
5. Set a **Port** value used by torrent peers to upload files from your px12-400r.
   The port value should be a number between 6881 and 6999, and your router must be configured to allow port forwarding on the same port. Refer to Configuring your router for torrent downloads for more information on how to do this.
6. Click **Apply** to save your changes.

Deleting torrent jobs

1. On the Torrent Download page, select a torrent you want to delete.
2. Click the under the Action column to delete the torrent.
3. Click **Yes** to delete the torrent.

Configuring Your Router for Torrent Downloads

You must manually configure your router to forward a specific port to your px12-400r. Most routers refer to this as port forwarding or application access, and it is recommended that you refer to your router's documentation to learn how to set these values.

Port Information Used to Configure Your Router

The following information may be required to manually configure your router:

Forward the port to your px12-400r IP address identified in the table:

Device IP Address

192.168.1.1

Port name

HTTP

Port number

Set to the same port value set on the Torrent Download page.

Protocol

TCP

Torrent Active Folders

Sharing Torrent Downloads with Other Peers

Torrent downloads allow you to share files using a peer-to-peer file sharing protocol. With Torrent Download, you can download files using the torrent protocol to your px12-400r and then those files can be uploaded by other torrent users.

Refer to Managing Shares for more information on managing Shares and Active Folders.

Configuring a Torrent Active Folder

1. From the Iomega StorCenter px12-400r Console, click **Shares**.
2. Select a Share to use as a Torrent Active Folder, and click to expand the Active Folder section.
3. Check **Enable**.
4. Select **Torrent** from the drop-down menu.
5. Click **General torrent settings** to set up Torrent settings. Refer to Torrent Downloads for more information on configuring your Torrent downloads.
6. Click **Apply** to save your changes.
7. Click **View Content** to see the files in this Share.

How do I...

manage a Share

Adding Torrent Files to Your px12-400r

1. Open the Shares page.
2. Expand the Share that is enabled as a Torrent Active Folder. Any Share can be enabled as a Torrent Active Folder. For information on enabling a Torrent Active Folder, refer to Torrent Active Folders.
3. Copy the downloaded torrent file to the Torrent Active Folder Share. The torrent file immediately starts to download to the Share. An administrator user can monitor its download progress on the Torrent Download page. All users can monitor the download progress through the Content Viewer on the Torrent Share.

Managing Torrent Downloads

In the Content Viewer, you can perform the following actions on torrents:

- Pause or resume a torrent job. Click to pause a torrent download. When a torrent download is paused, you can resume the download by clicking .
- Delete a torrent job. Click to delete the torrent download.

Videos

Video Capabilities Overview

Your Iomega StorCenter has multiple ways to manage your videos.

Your Iomega device can:

- Stream movies that are in Shares with media sharing enabled
- Upload videos that are added to Shares associated with social media sites

---

How do I ...

stream movies
share movies through social media

Streaming Movies

The Iomega StorCenter has a built-in media server that, when turned on, scans for movies in specific folders that have media sharing enabled. Any movies contained in these specific folders are accessible to any user on your network with a media player. For information on enabling a folder as a media folder, refer to Managing Shares.

Scanning for Movies

The Media Server automatically scans for media content on a regular basis. However, you can click **Scan now** at any time to force the media server to perform an immediate scan for movies. This is especially useful after you have created new folders with media sharing enabled and copied a large amount of media content to them.

Adding Applications to Your Device

Application Overview

You can install supported applications on your px12-400r using the Application Manager page. For each application installed you may have the option to uninstall, start, and stop the application.

How do I...

install an application

Application Manager

The Application Manager page allows you to add applications to your px12-400r from an installation file located on your computer. For each application installed you may have the option to uninstall, start, and stop the application. This page shows the applications which came preinstalled with your px12-400r, as well as applications that you have manually installed.

Note: Only valid applications built using the Iomega StorCenter SDK can be installed on your px12-400r.

Starting or stopping an application

When available, click in the Action column to stop an application. Click to start it again.

Adding applications

1. Click the **Add application** link. The Add application window displays.
2. Enter the path and name of the application file, or click **Browse**, and select the application file located on your computer.
3. Click **Upload** to install the application.

Removing applications

When available, click in the Action column to uninstall an application.

How do I...

enable security

Upgrading Your Device

Software Updates

The Software Updates page identifies the px12-400r software status and provides the ability to update the software for the px12-400r.

This software is protected by RSA BSAFE technology.

1. In the table listing the current software installed on your px12-400r, click in the Action column to check for updates.
2. The Status column will state whether the software is up to date or if an update is available.

   To copy an update file to your px12-400r, click . The software update file is downloaded directly to your px12-400r.

3. If multiple updates are ready, you may install all the updates at the same time. Click **Apply all pending updates** to install the available updates. The software updates are applied to your px12-400r.

4. Once the software is installed, the px12-400r will reboot. If you are applying multiple updates, you only need to reboot once. Do not power down the px12-400r during this time.

5. If you want to remove the update without applying changes, click in the Action column.

Caution: Do not shut down the px12-400r during the update process as this can damage the px12-400r. The px12-400r will be temporarily inaccessible during the software update. Be sure no critical files are being accessed.

---

during this time.

Manual update process: installing a device software update

1. In the table listing the current software installed on your px12-400r, click in the Action column to check for updates.
2. If an update is available, the Status column will state that a software update is available with a link. Download the update file to your local computer.
3. To retrieve the update, click **Add Software**.
4. In the **Add Software** pop-up window, if an update is available, there will be a link to download the appropriate update for your px12-400r. Click the link, follow the instructions on the download site page, and download the software update to your local computer.
5. Once downloaded, click **Browse** to select the update, and then click **Upload** to continue.

   When the update is uploaded to the px12-400r, the Status column will say **Ready to apply**.

6. Click **Apply all pending updates** to apply the update or updates. The software updates will be applied to your px12-400r. If you want to remove the update without applying changes, click in the Action column.

   The px12-400r restarts once the software is installed. You should not power down the px12-400r during the installation process as this can damage the px12-400r. If multiple updates are ready, all of them will be applied, requiring only one reboot.

   Caution: The px12-400r will be temporarily inaccessible during the software update. Be sure no critical files are being accessed.

Recovering Your Device Configuration

Copying Your Iomega StorCenter px12-400r Settings to Other Devices

The Configuration Backup and Restore page allows you to back up and restore system configuration information. Backing up a configuration saves various system properties, including users, groups, device identification, and Share names and permissions. Configuration information is saved to a file, and you can save as many versions of the file as you want. After backing up the configuration, you can restore it to your px12-400r at any time. You can also apply the configuration backup to other Iomega StorCenter devices of the same model, effectively using the configuration as a template.

Note: Configuration Backup and Restore does not back up or restore any data files on your px12-400r.

Backing up Device Configuration

1. On the Configuration Backup and Restore page, click **Back up configuration** to select a name and location for your configuration backup.
2. Save the configuration file to an external device, such as your computer or a USB drive. You can save as many configuration backups as you want.

Restoring a Configuration Backup

1. On the Configuration Backup and Restore page, click **Restore configuration** to select a saved configuration backup.
2. In the Restore Configuration dialog box, click **Browse** to locate a previously saved configuration backup stored on your computer or USB device.
3. Select one of the following options:
    - **Restore settings** — overwrites any existing settings, such as device identification and Share names. When you select this option, existing data on the px12-400r is not deleted, and the configuration restore operation starts automatically after you click Apply in the Restore Configuration dialog box.
    - **Restore settings and drive configuration** — deletes all data, users, and settings from the target px12-400r. If you select this option, a confirmation dialog box displays and informs you that restoring the configuration will delete all data and overwrite any existing users or settings on the target px12-400r. Check **Check this box to continue** to confirm this dialog box or click **Cancel** to stop the configuration restore process.
4. Click **Apply** to save your changes. After you click Apply, the restore process starts.
5. If your source px12-400r had Active Directory enabled, you are prompted to enter the administrator name and password of an account that has the rights to join the domain.
6. Click **OK**.

Hardware Management

About the Iomega StorCenter px12-400r Components

This topic describes the front and rear panel components of the px12-400r.

Front Panel

Status Indicators, Buttons and Ports

1. Power button — Press and release to power the px12-400r on or off. When the px12-400r is powered up, pressing the power button for less than 4 seconds will result in a graceful system shutdown.

CAUTION! Holding the power button for 4 seconds will result in a forced shutdown and could cause data loss if data transfers are in process.

2. Power / Status Indicator —

- Solid blue — unit is powered on; no faults
- Flashing blue — unit is initializing/booting or shutting down
- Flashing amber — indicates a system failure: power supply, fan failure, or drive failure. Use the device console to view details.

3. Drive bays — The Iomega StorCenter px12-400r has 12 user-serviceable drive bays. See Drive Bay Detail below for additional information.

4. USB 2.0 connector — Supports devices such as USB storage devices and printers.

Drive Bay Detail

1. Drive Sled Release Latch — Press the release button and pull the latch to release the drive sled.

Refer to the list of qualified hard disks on the Iomega support site at www.iomega.com/nasdisks before adding new drives.

2. Drive Status Indicator —

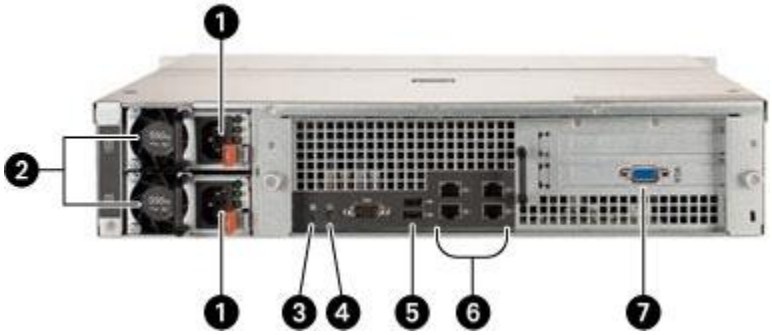
- Solid blue — drive at speed; no faults
- Flashing blue — drive is in RAID rebuild mode
- Solid red — drive failure.
- Off — drive is spun down in energy-saving mode

3. Drive Activity Indicator —

- Flashing white — activity in process for the drive's RAID set
- Off — no activity to the drive's RAID set

Rear Panel

.



1. AC Power Connectors — Connect both AC power connectors to an Uninterruptable Power Supply (UPS) to provide redundant power for your px12-400r. The AC power supply will automatically switch to the correct voltage for your region.

2. Power Supply — The px12-400r has redundant hot-swappable power supplies. If one power supply fails, the other power supply will immediately take over. For maximum time-up, a failed power supply can be replaced while the px12-400r is running.

3. System ID LED — Flashes blue when the Blink Lights feature is enabled in the Iomega StorCenter px12-400r Console. This light is used to identify a specific px12-400r in installations with multiple devices.

4. Reset Button — Press the Reset button to reset security and network settings. This allows you to regain access if network settings are incorrect or you've forgotten your password. Note: The Reset button does not initiate a full factory reset. To perform a full factory reset, select Factory Reset from the System page in the Iomega StorCenter px12-400r Console

5. USB 2.0 connectors — Supports devices such as USB storage devices and printers.

6. Gigabit Ethernet Ports — High-speed Ethernet connectors that automatically detect your network speed (10/100/1000Base-T).

7. VGA output connector — Connect a monitor for video surveillance applications.

Default Settings:

- IP Address: If not DHCP server is found on your network, the StorCenter will get a self-assigned IP address in the 169.254.x.x range.
- Device Name: The default name for your Iomega StorCenter px12-400r is px12-400r-XXXXXX (where XXXXXX is a unique string of letters and numbers).
- Default Shares: Backups, Documents

.

Energy Saving

The Energy Saving page provides power settings for the px12-400r.

Power Down Drives

Click the Power Down Drives drop-down menu to select how much idle time should be allowed to elapse before the px12-400r powers down the drives. Drives automatically power back up when the px12-400r accesses them. You may notice a slight delay when the drives are accessed.

Brightness

To adjust the brightness of the lights on the px12-400r, set the **Indicator Brightness** to High, Medium, or Low.

Wake On LAN

Wake On LAN powers on your px12-400r when a specific signal is sent over the network. Additional software may be required to send the Wake On LAN signal to your device.

1. Check the **Wake On LAN** checkbox to enable Wake On LAN.
2. Click **Apply** to save your changes.

Creating A Power Schedule

You can create a power schedule to turn your px12-400r on and off. Power off and Power on functions can be scheduled as one-time events, or recurring events. When you create a power schedule, you can set the day and time to power down the device. In addition, you can optionally set power on times.

1. Check the **Enable device power schedule** checkbox.
2. Select the days for your px12-400r to power on or off.
3. Set the power schedule time in both hours and minutes (HH:MM), and specify AM or PM.
4. Click **Apply** to save your changes.

Factory Reset

Factory Reset returns the px12-400r to its original state. This feature is useful if you give your px12-400r to someone else.

Factory Reset provides two options for returning your px12-400r to its original state:

- **Quickly delete all data** — permanently deletes all record of existing or deleted data, users, and passwords.
- **Securely delete all data** — this option takes significantly longer, but provides an added security benefit by permanently erasing all data on the drives to prevent recovery of existing or deleted data, users, and passwords. The secure delete operation renders all data irrecoverable.

Note: You can use the factory reset feature only to erase the drives internal to the px12-400r. You cannot use this feature to reset any external storage devices that may be connected.

1. Choose one of the following options:
    - Quickly delete all data
    - Securely delete all data
2. From the **After Reset** drop-down menu, choose to **Restart** or **Power off** the px12-400r after the factory reset completes.
3. Click **Apply**.
4. In the pop-up confirmation, click **Yes** to perform the factory reset. After the factory reset completes, the px12-400r powers down or restarts depending on your selection.

Warning: When you quickly delete or securely delete all data on your Iomega StorCenter, any installed applications, as listed on the Application Manager page, are also deleted. Go to www.lifelineapps.com to download and reinstall your applications. In addition, you should visit the Iomega support web site for specific information on reinstalling applications that came preloaded with your px12-400r.

UPS Management

The Iomega StorCenter UPS Management page allows you to monitor the status of an attached Uninterruptible Power Supply.

If your px12-400r is connected to a UPS battery backup unit, it is listed on this page. The battery status of the backup unit is also indicated, displaying how much of a charge is left in the battery. To monitor the battery status of your UPS unit, connect your px12-400r to it with a USB cable.

If the px12-400r is running from the UPS battery, it automatically shuts down to preserve data as the battery charge gets low.

Adding New Drives to Your Iomega StorCenter px12-400r

To install new hard drives in your px12-400r:

1. Before installing a new hard drive in your px12-400r, check the hard drive compatibility list online at www.iomega.com/support for approved and supported hard drive brands and models.

2. Mount the drive carrier containing the new drive in an available slot.

3. A confirmation dialog box displays as soon as the px12-400r detects the new hard drive. Click **Yes** to proceed.

   Note: All data on the drive is deleted.

4. You are re-directed to the Iomega StorCenter px12-400r Console.

5. Access the **Drive Management** page.

   Your px12-400r displays the new hard drives in the bays they are mounted in.

6. To create a RAID Array, you must install a minimum of two hard drives. The same confirmation dialog box displays. Click **Yes** to proceed.

   Note: You can create a Storage Pool using one hard drive if desired. You will not have any RAID protection options and can only select **None** from the RAID dropdown list while configuring your Storage Pool.

7. When all new drives are detected, click **Add a Storage Pool**.

8. Complete the Storage Pool configuration options and select the desired drives on which to build the Storage Pool by checking the boxes next to them. All drives in a Storage Pool must be the same model, manufacturer, and capacity.

9. Allow a few minutes for the RAID array and Storage Pool to build. When complete, the Storage Pool status displays on the Drive Management page.

Troubleshooting Routers

If you encounter a problem while connecting or using your px12-400r, check the topics listed below for possible solutions.

If you have properly set port forwarding on your router and remote access still does not work, you may have multiple routers on your network. In this situation, you will most likely have two NAT (Network Address Translation) this situation you will most likely have two NAT (Network Address Translation) firewalls.

1. One of the easiest ways to identify this issue is to log in to the router to which the px12-400r is connected.
2. Once you have logged in, go to the page that shows the router's WAN IP address, usually Status or Network Info.
3. If the WAN IP address begins with 192.168, 10, or 172, you may have a NAT Firewall between the router and internet connection.

There are several options for resolving double NAT situations. The sections below explore the pros and cons of each resolution:

> These instructions will refer to the router that is connected directly to the internet as the Primary Router. The cascaded router or router to which your px12-400r is connected is referred to as the Secondary Router.

- Use the primary router's DMZ
- Port forward the primary router to the secondary router
- Put the secondary router in bridging mode
- Put the primary router in bridging mode

Enabling the DMZ

Most routers have a feature called DMZ or Default Server. DMZ stands for Demilitarized Zone, Data Management Zone, Demarcation Done, or Perimeter Network. The DMZ allows you to enter an IP address that will exist outside the router's NAT Firewall.

This is the easiest way to configure your network to handle double NAT situations; however, it is dependent upon DMZ functionality within your primary router.

To enable the DMZ:

1. Log in to the primary router.
2. Navigate to the settings page for DMZ or Default Server. Refer to the documentation that came with your router for information on where this feature is found.
3. Enter the secondary router's IP address.
4. Save your settings.

Your secondary router is no longer behind your primary router's firewall. If port forwarding is correctly configured, remote access should now be working properly. Moving your secondary router into the DMZ should not have any effect on the security of the network, since it is still protected by the secondary router's firewall.

Configuring Port Forwarding on Double NAT Networks

If for some reason the network configuration cannot be changed and your setup requires the double NAT, you must perform the port forwarding steps twice. On the primary router, set the port forwarding to the cascaded router's external IP address. On the cascaded router, set the port forwarding to the px12-400r's IP address.

Bridging the Secondary Router

Bridging the Primary Router

If none of the above options are available, you must enable transparent bridging on your primary router. This may require contacting your ISP (Internet Service Provider) to configure the DSL or Cable Modem/NAT into bridge mode, which then disables the first NAT/Firewall. After this first firewall in the modem is disabled, the secondary router handles all the network traffic, Port Forwarding, and allows Remote Access to work.

> You should not attempt bridging without help from the ISP. If bridge mode is attempted by the customer and not configured properly, it can render the customer's internet connection inoperable. Primary router bridging may also require special configuration information and settings on the secondary router.

If you configured your px12-400r using DHCP, you may not be able to reconnect to it via Remote Access after a reboot. DHCP automatically receives an IP address from the server whenever the px12-400r restarts. This is a very simple way to configure the px12-400r but can cause problems with your router's port forwarding settings. The router does not dynamically update port forwarding settings and cannot port forward to your px12-400r if its IP address changes.

To resolve this problem, try one of the following processes:

- Increase the length of the DHCP lease: Your router attempts to remember all DHCP clients and assigns them the same IP address every time they request an IP address; however, the router forgets clients if they do not request an IP address for a certain amount of time. Your router has a setting for the duration of the validity of the DHCP lease. If your network requires DHCP, this may be a good solution; however, it is not always guaranteed to work. Occasionally updating your router's port forwarding settings may be required.
- Use Static DHCP: Some routers allow you to assign Static IP addresses through the DHCP system based on the MAC address of the device. This ensures that the px12-400r always gets the same IP address, and your port forwarding settings are always correct. Static DHCP allows you to leave your px12-400r in DHCP mode. Refer to your router's documentation for more information on configuring DHCP settings.
- Use a Manual IP Address: Changing the Manual IP address reduces the reliance of your px12-400r on the DHCP server; however, you must perform additional configuration for it to work properly.
    1. Log in to your router and write down the DHCP range it is using.
    2. Refer to your router's documentation for more information on configuring DHCP settings.
    3. Navigate to the IP address settings interface page on your px12-400r . For more information, check the Network Settings section of this manual.
    4. Enter a new IP address that is outside of your router's DHCP range. For example, if your router is distributing IP addresses in the range of 192.168.14.2 through 192.168.14.50, you must assign the px12-400r a number between 192.168.14.51 and 192.168.14.255.

Make sure you are assigning the px12-400r an IP address that is not in use by another device.

5. Enter a subnet mask. The subnet mask describes the size of your network. For most networks this is 255.255.255.0 which allows for 256 network devices. If you are on a larger network or are using the self-assigned APIPA range (169.254.x.x), you must use a 255.255.0.0 or larger subnet mask.
6. For best results, enter the IP address(es) for your DNS Server(s).
7. If necessary, enter the IP address(es) for your WINS server(s).
8. Enter a gateway address. In most cases, this is the IP address of your router.
9. If necessary, update your router's port forwarding information with the new static DHCP IP address.

Additional Support

How to Get Help

Iomega is committed to providing excellent customer support. To meet this goal, Iomega offers a variety of support options designed to meet the needs of a wide range of users. For complete information on the support options available for your Iomega product, visit the Iomega website. Please select your region carefully.

Here's just some of what is available on Iomega's award-winning web support site 24 hours a day, 7 days a week:

- Answers to frequently asked questions (FAQs)
- Online help pages with troubleshooting or basic how to information
- Up-to-date Iomega software and drivers
- Advanced online support options, such as 1-on-1 live chat and email
- Electronic copies of Iomega product manuals
- Information on telephone support options
- Information on advanced technical service options, such as data recovery
- Warranty information and product return instructions

Support options available may vary depending on your region and language of choice. Iomega's specific customer support policies (including fees for services) and procedures change as technology and market conditions dictate. To obtain information about Iomega's current policies, please visit our website at:

www.iomega.com/supportpolicy.html

or write to:

Iomega Customer Service
4059 South 1900 West
Roy, UT 84067, USA

Support

The Support feature opens the Iomega web site where you can get more information about your Iomega StorCenter px12-400r. The Support page provides access to content for learning more about using and supporting your px12-400r.

Refer to the Iomega Support site for more information.

Legal

px12-400r Trademark Page

Iomega, the stylized logo, and StorCenter are either registered trademarks or trademarks of Iomega Corporation in the United States and other countries. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Mac, Macintosh, and AppleTalk are registered trademarks or trademarks of Apple Computer Inc. in the United States and/or other countries. Certain other product names, brand names, and company names may be trademarks or designations of their respective owners.

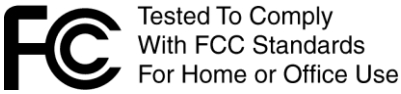
© 2012 Iomega Corporation. All rights reserved.

Regulatory Information

This topic provides regulatory information for various countries.

FCC (United States)

The computer equipment described in this manual generates and uses radio frequency (RF) energy. If the equipment is not installed and operated in strict accordance with the manufacturer's instructions, interference to radio and television reception might result.



This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Note: Changes or modifications to the electronics or enclosure of this product must be expressly approved by Iomega; otherwise, the user's authority to operate this product might be voided by the FCC.

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Canadian Verification

This Class A digital apparatus complies with Canadian ICES-003. Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

CE (European Community)

Iomega declares that this Iomega product conforms to all applicable European Directives and Standards, including by way of example, 2004/108/ EC, 2009/125/ EC, and 2006/95/ EC. The Declaration of Conformity can be obtained by contacting Iomega or is available at www.iomega.com/support/ce.

Manufacturer/Responsible Party

Iomega Customer Service, 4059 South 1900 West, Roy, UT 84067

EU Representative

Iomega International SA
H/O Iomega Netherlands
3821 BM Amersfoort
NL - The Netherlands

RoHS COMPLIANT

Waste Electrical and Electronic Equipment (WEEE)

In accordance with European Directive 2002/96/EC on Waste Electrical and Electronic Equipment (WEEE), the presence of the above symbol on the product or on its packaging indicates that this item must not be disposed of in the normal unsorted municipal waste stream. Instead, it is the user's responsibility to dispose of this product by returning it to a collection point designated for the recycling of electrical and electronic equipment waste. Separate collection of this waste helps to optimize the recovery and recycling of any reclaimable materials and also reduces the impact on human health and the environment.

For more information concerning the correct disposal of this product, please contact your local authority or the retailer where this product was purchased.

Safety Information

Observe the following guidelines when using your Iomega StorCenter px12-400r:

1. Follow all instructions marked on the px12-400r and in the documentation.
2. Use only the power supply cables provided with the px12-400r.
3. Unplug the px12-400r before cleaning. Do not use liquid or aerosol cleaners. Use a damp cloth for cleaning.
4. Do not use the px12-400r near water. Do not spill liquid on or into the px12-400r.
5. Do not place the px12-400r on an unstable surface.
6. Do not place the px12-400r near or on a radiator or heat register.
7. Openings in the px12-400r are provided for fans and air ventilation and should not be blocked or covered. Make sure the px12-400r has ample ventilation (at least 6 inches or 127 mm) in front and behind the unit.
8. Do not walk on the power cord or allow anything to rest on it.
9. There is a danger of explosion if the battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the equipment manufacturer. Dispose of used batteries according to local, state, regional, and federal regulations.

Under any of the following conditions, unplug the px12-400r from the wall outlet and contact technical support:

- The power cord or plug is damaged.
- Liquid has been spilled into the device.
- The device does not function properly when the operating instructions are followed.
- The device was dropped or the exterior enclosure is damaged.

Limited Warranty

Drives and Media

- Coverage
- Excluded Products and Problems
- Remedies
- Obtaining Warranty Service
- Limitations

Coverage

Iomega warrants this hardware product to be free from defects in materials and workmanship for the warranty period. This non-transferable, limited warranty applies only to you, the first end-user purchaser. The warranty begins on the date of purchase and lasts for a period of one (1) year for products purchased in the Americas, the Asia-Pacific region, or non-European Union nations in Europe, the Middle East, or Africa; ninety (90) days for Iomega reconditioned products purchased in these regions; or, two (2) years for products purchased by an end-user in member nations of the European Union. Customers who register their new products at www.iomegareg.com within 90 days of purchase will receive a warranty extension so that their total warranty shall be a period of three (3) years in all regions. Reconditioned products are not eligible for a warranty extension.

Excluded Products and Problems

This warranty does not apply to: (a) software of Iomega or any affiliates; (b) expendable components such as fuses or bulbs; or (c) third party products, hardware or software, distributed by Iomega. Iomega makes no warranty of any kind on such products which, if included, are provided "AS IS." This warranty also excludes damage caused by accident, misuse, abuse, use of non-Iomega approved media or replaceable components, exposure of media to excessive magnetic fields, or external environmental causes, or damage arising from any cause or causes for which Iomega is not responsible such as exposure to abnormal temperatures, shock, power surges, power outages, improper power supply, or damage caused while the product is being shipped from you to Iomega.

Your Iomega product may contain certain replaceable components such as hard drives or power supplies. Refer to your product documentation or contact Iomega to determine whether specific components are replaceable. Any alteration, change, modification, or repair (other than replacement of a replaceable component) made to the product by a party other than Iomega or Iomega's authorized service provider will void this warranty.

All Iomega products are manufactured solely to standard commercial grade levels of reliability and are not intended for use in any systems that require Iomega products to conform to the higher grades of reliability, such as critical safety systems, life-support systems, medical devices, nuclear facilities, military devices, satellites, or aviation equipment. Iomega shall not be liable for any damages incurred if Iomega products are used in such capacities, and no warranty shall apply.

Remedies

Your sole and exclusive remedy for a covered defect is repair or replacement of the defective product, at Iomega's sole option and expense (shipping may be charged), and Iomega may use new or refurbished parts or products to do so. If Iomega is unable to repair or replace a defective product, your alternate exclusive remedy shall be a refund of the original purchase price.

The above is Iomega 's entire obligation to you under this warranty. IN NO EVENT SHALL IOMEGA BE LIABLE FOR INDIRECT, INCIDENTAL, CONSEQUENTIAL OR SPECIAL DAMAGES OR LOSSES, INCLUDING LOSS OF DATA, USE, OR PROFITS EVEN IF IOMEGA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall Iomega 's liability exceed the original purchase price of the drive or the media disk. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

Obtaining Warranty Service

You must notify Iomega within the warranty period to receive warranty service. Just as technology and market conditions vary, Iomega's specific customer support policies (including fees for services) and procedures change over time. To obtain information about Iomega's current policies or warranty service, please visit our website at www.iomega.com/supportpolicy.html or write to:

Iomega Customer Service, 4059 South 1900 West, Roy, UT 84067

Contact information for Iomega Customer Service can be obtained on our support website at:

- Americas www.iomega.com/support
- Europe www.iomega.com/europe/support
- Asia www.iomega.com/ap/support

If your product is eligible for warranty service, you will be required to return it to Iomega, along with proper identification, a return authorization number obtained from the Iomega website or provided by the Iomega representative, and proof of purchase. Iomega will not protect, recover, or return data during warranty service, so you should duplicate your data before shipment.

Limitations

THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED. To the extent permitted by applicable law, IOMEGA SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Any implied warranty required by applicable law shall be limited in duration to the express warranty term. Some jurisdictions do not allow disclaimers of implied warranties or limitations on how long an implied warranty lasts, so the above limitation may not apply to you.

This warranty gives you specific legal rights, and you may also have other rights that vary from jurisdiction to jurisdiction. Any suit for breach of any warranty on your product must be filed within one (1) year of the first date the suit could have been brought.

Open Source

The software included in this product contains copyrighted software that is licensed under open source agreements. Components of this software covered under GPL or other open source licenses are fully documented as to license and redistribution requirements in the ReadMe file available with the source code. The corresponding source code package is available for download from Iomega's Support and Download site at www.iomega.com/support. To locate the download page for open source code, select your Iomega product and your operating system. Scroll down the page to the search field and enter "open source". In addition, you can also obtain a copy of the applicable open source code on CD by sending a money order or check for $10 (USD) to:

Iomega Corporation • ATTN: Source Code • 4059 South 1900 West • Roy, UT 84067 USA

Please include the model name for your Iomega product with the request.